



INSTITUTE FOR DEFENSE ANALYSES

**The Development of RAPID System:
From Concept to Initial Use and Beyond
Status Report**

L. B Scheiber, Project Leader

February 2006

Approved for public release;
distribution unlimited.

IDA Document D-3249

Log : H 05-002148

This work was conducted under Purchase Orders ME1100, 1101, and 1102 for the Delaware River Maritime Enterprise Council (DRMEC). The publication of this IDA document does not indicate endorsement by the Department of Defense, nor should the contents be construed as reflecting the official position of that Agency.

© 2005, 2006 Institute for Defense Analyses, 4850 Mark Center Drive, Alexandria, Virginia 22311-1882 • (703) 845-2000.

This material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at DFARS 252.227-7013 (NOV 95).

INSTITUTE FOR DEFENSE ANALYSES

IDA Document D-3249

**The Development of RAPID System:
From Concept to Initial Use and Beyond
Status Report**

L. B. Scheiber, Project Leader

M. H. Anstice

J. E. Hartka

J. J. Karrels

P. N. Miller

E. R. Smothers

PREFACE

The Department of Defense moves a great deal of war materiel between the forts in the United States and its military elements overseas. Much of this materiel is moved by a supply chain consisting largely of trucks, trains, and ships. Trucks and trains carry materiel over land routes, for example, between forts and ports; ships carry it between ports. The Federal Government, including the DoD, along with law enforcement organizations such as local police departments and port security, has been working to increase the security and accountability of this supply chain. Still needed, however, are adequate capabilities for tracking individual pieces of cargo, e.g., vehicles and shipping containers, in order to provide a common operating picture to all stakeholders and to alert stakeholders in the event of an occurrence of an adverse incident.

In 2003, the Maritime Administration of the Department of Transportation tasked IDA to initiate an effort to help identify solutions to the above noted problem areas (Task Order EF-1-2295). In 2004, the Delaware River Maritime Enterprise Council (DRMEC) tasked IDA to initiate the design and development of an online system to send alerts to the stakeholders (ME1100). In 2005, this tasking was increased to include the design, development, and demonstration of a pilot version of an online system to support the tracking of individual pieces of cargo, to provide

a common operational picture to all stakeholders, and to provide a means of alerting the stakeholders (ME1101). Additional tasking was provided to further identify advanced features for the system (ME1102). This document is being provided at the request of DRMEC to bring together in one place the significant elements of the various briefings and other material provided during the efforts associated with the above tasks.

The IDA team consisted of Dr. Lane B. Scheiber, Project Leader, Mr. Michael H. Anstice, Dr. Joseph E. Hartka, Mr. Jeffrey J. Karrels, Mr. Philip N. Miller, and Mr. Ernest R. Smothers. The team wishes to acknowledge the immense benefit derived from the comments by those who reviewed the briefing including, ADM Dennis C. Blair, USN (Ret.), Mr. Philip L. Major, Ms. Ruth L. Greenstein, Dr. George E. Koleszar, Dr. John R. Shea, Dr. Richard J. Ivanetich, General Hansford T. Johnson, USAF (Ret.), and those who provided comments on this document, Dr. Thomas L. Allen, Dr. William L. Greer, Dr. Gregory N. Larsen, Dr. Daniel Y. Nakada, and Dr. John R. Shea. Many thanks also go to IDA/SED's production staff, notably Ms. Patricia G. Phillips, Mrs. Patricia Hatter, and Ms. Diane O. Wright, for their outstanding assistance.

(This page is intentionally blank.)

TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	1
BRIEFING REPORT	5
A. Background	6
B. IDA Tasking	12
C. Initial Design	14
D. First Demonstration	18
E. Second Demonstration	36
F. Potential Next Steps	50
1. First Steps.....	50
2. Making a Case for Virtual Collaboration	50

Appendixes

- A. The DRMEC Organization
- B. Information Distribution Support System
- C. Additional Views From the First Demonstration
- D. Improving Disaster Response Through Collaboration
- E. Glossary

(This page is intentionally blank.)

EXECUTIVE SUMMARY

A. BACKGROUND

The Federal Government has been working to increase the security of U.S. ports, which includes the supply chains that move the goods and materiel that pass through these ports. This is especially true in the case of war materiel moving between the forts and depots in the United States and the theaters of operation.

Many organizations are involved in improving the security of military shipments including a large number of law enforcement organizations. However, there has been no means of providing these participants with a common operating picture. Thus, coordinating efforts to ensure prompt and safe delivery has been difficult at best. Knowledge of where cargo is and when it will enter one's jurisdiction is of paramount importance to enable its safe movement. The current process also lacks a communications system that can quickly get security alerts into the hands of those who need them to respond to critical situations.

B. EVOLVING SITUATION

Following the attacks of 9/11, the Delaware River Maritime Enterprise Council (DRMEC), a Pennsylvania not-for-profit organization, turned its attention to these problems. As a result, DRMEC, along with the Maritime Administration

of the Department of Transportation (MARAD), the Philadelphia Regional Port Authority (PRPA); federal, state, county and city law enforcement; military; homeland security; and commercial organizations began to identify and establish first-order mechanisms for sharing information among the stakeholders. As part of this effort, DRMEC developed the concept of a center, called Regional Agile Port Intermodal Distribution (RAPID) Center, for managing the collection and distribution of the information pertaining to the movement of war materiel.

C. IDA TASKING

In 2003, MARAD tasked IDA to initiate an effort to help identify approaches to improve the safety and accountability of war materiel moving between the forts and the ships at the port of Philadelphia. In 2004, DRMEC tasked IDA to initiate the design and development of an online, wide area network system to enable RAPID Center to send alerts to the stakeholders. In 2005, this tasking was increased to include the design, development, and demonstration of a pilot version of an online system to support the tracking of individual pieces of cargo, to provide a common operational picture to all stakeholders,

and to provide RAPID Center a means of alerting stakeholders to the occurrence or potential occurrence of significant events. Tasking to identify advanced features for the system was also included.

D. IDA'S EFFORT

The effort included the design and development of automation, called RAPID System, to support RAPID Center as well as the communications necessary to provide alerts to the stakeholders. The system also provides online information to stakeholders to enable them to all work from the same operational picture.

The initial version of the system has been developed using IDA's Internet-based Information Distribution Support System (IDSS) concept. It has four DRMEC modules—one each for logistics, security, reports, and images.

The *logistics module* contains the list of cargo to be moved between the forts and the ship. It differs from a cargo manifest in that it contains information on where each item is and how it is being transported over land. Each item of cargo contains an identification (ID) tag that is scanned each time the item's Transportation status changes, e.g., taken off the ship or placed on a truck. RAPID System contains an automated means of processing this scanned information to keep the cargo list updated.

The *security module* contains the capability to send alerts—especially concerning critical security issues—to users who have a need for information referenced by the alert. An example of this could be a terrorist event that would affect the cargo's movement. The initial effort provides two communications means for sending out alerts.

They can be sent to wireless devices, such as mobile phones, or to email addresses. Users can specify their preferred means for receiving the notifications.

Because of the potential sensitivity of the information, the text of the alert acts as a pointer to the location of the information in RAPID System. To view that information, users must connect to the RAPID System website by way of a secure link. The connection to the website can be accomplished using one's mobile phone and other mobile devices as well as a personal computer (PC). Alerts can also contain attachments that can be text, pictures, or maps. Although attachments can currently be viewed only when viewing the alert from a PC, they should shortly be displayable on mobile phones and other mobile devices.

RAPID System collects and maintains data on the status of the transmission to each wireless device with which it communicates over the Cingular network. The data include the date and time the alert was sent from RAPID System, when it was sent by the service provider to the phone, and when it was read. An online report is available to enable the sender of the alert to check its delivery status.

The *reports module* has the capability to store and provide ready reference to reports that RAPID Center generates and places in RAPID System.

The *imagery module* has the capability to store and provide ready access to the many different types of imagery received or generated by RAPID Center including streaming video.

E. INITIAL DEMONSTRATIONS

In FY 2005, RAPID System was used to support RAPID Center in two movements of war materiel through the port of Philadelphia. In the first demonstration, the system supported the redeployment (return from theater) of 733 items of equipment from overseas to 16 destinations, which included depots and home stations of the units that “own” the equipment. In the second demonstration, it supported the deployment (move to theater) of the 10th Mountain Division from Fort Drum, NY, along with the movement of additional cargo from several other forts (1,029 items total). RAPID System performed as designed in both demonstrations.

Although RAPID Center used RAPID System to send many security alerts during the two demonstrations, several in particular provided opportunities to demonstrate the quickness with which the alert system works. These included alerts for a bomb on train tracks, the crash of a small plane,

and the London bombings. The London bombings alert was of particular importance as a train loaded with war materiel was nearly ready to depart Fort Drum. Using RAPID System, the stakeholders were quickly able to ascertain the train’s location and keep it and its cargo secure until the true nature of the threat could be determined.

F. CONTINUED DEVELOPMENT AND UTILIZATION

RAPID System is a spiral development effort. Following each demonstration, new features are added and existing ones are upgraded. For example, it is expected that the system will, in the near-term, need to simultaneously support multiple ships at multiple ports. Efforts are currently underway to determine system changes necessary to accommodate this expansion.

Further, RAPID Center is the center of an information hub with many of the organizations that would need to respond to a disaster able to connect to its RAPID System. This places RAPID Center in a good position to support the collaboration necessary for the responders to coordinate their efforts to bring about rapid and efficient responses. Modifications are being made to RAPID System to enable RAPID Center to demonstrate a virtual collaboration capability when it supports the movement of war materiel in the future.

(This page is intentionally blank.)

BRIEFING REPORT

BACKGROUND

A. BACKGROUND

This section begins by describing the basic operational problem that confronts many organizations concerned with the deployment, redeployment, and sustainment of U.S.

military forces. It then briefly describes the formation of an organization to address the problem, and concludes with a discussion of IDA's involvement and the tasking that motivated the work addressed in this report.

BACKGROUND

THE OVERALL PROBLEM

Since 9/11, the Federal Government has been working to increase the security of U.S. ports and the supply chains that provide goods and materiel that pass through these ports. This is especially true in the case of war materiel moving between the forts in the United States and the theaters of operation. Numerous factors impede the secure, efficient, timely, and accountable movement of this materiel. Examples of these are shown here.

Although many organizations are involved, including a large number of law enforcement organizations, there has been no viable means of providing these shareholders with a common operating picture. Thus, coordinating efforts—for example, on cargo that requires special handling and, in particular, that which needs law enforcement protection—has

been difficult at best. Knowledge of where cargo is and when it will enter one's jurisdiction is of paramount importance to enable its safe movement. The current process also lacks a communications system, which can quickly pass security alerts to those who need to respond to critical situations.

An additional factor is that the Military Surface Deployment and Distribution Command (SDDC) of the Department of Defense's Transportation Command (DoD's TRANSCOM) is under pressure to outsource portions of the process of moving the war materiel. However, before this can be done, a more formal and better documented set of procedures must be established.

THE OVERALL PROBLEM

Numerous factors impede the secure (against terrorism), efficient, timely, and accountable movement of war materiel between forts and the theaters, for example:

- Inadequate asset visibility and transportation constraints have led to less-than-acceptable transit times, backlogs, and repetitive ordering of needed supplies
- Many organizations involved—no Common Operating Picture
- Inadequate coordination with other organizations that are or could be affected, such as law enforcement
- Military Surface Deployment and Distribution Command (SDDC) requires well-defined process to be able to outsource portions thereof

DRMEC

Established in 1999, the Delaware River Maritime Enterprise Council (DRMEC),¹ following the attacks of 9/11, turned its attention to solving some of the problems associated with the secure, effective, and efficient movement of war materiel. DRMEC along with the Philadelphia Regional Port Authority (PRPA) worked to establish a Seaport Security Working Group for the port of Philadelphia.

Stakeholders participating included federal, state, county, and city law enforcement, military, homeland security, and commercial organizations. As a result, DRMEC and PRPA began to identify and establish needed first-order information-sharing mechanisms among the stakeholders.

As a next step, DRMEC established the “RAPID International Security Knowledge Alert” (“R.I.S.K.

Alert™”) system, which provided stakeholders with sensitive commercial/homeland security information shared across the spectrum of law enforcement and military organizations. The information provided total visibility of cargo, crew, and vessel sailing from foreign ports to the United States.

Current efforts include “proof-of-concept” demonstrations of a center, called RAPID Center, for managing the collection and distribution of the information pertaining to the movement of the cargo along with the supporting automation. The demonstrations also include the communications necessary to provide alerts as well as online information for those who need it for action as well as to keep all stakeholders informed.

¹ Additional information about DRMEC is available in Appendix A.

DRMEC

- The Delaware River Maritime Enterprise Council (DRMEC), a Pennsylvania not-for-profit organization, is focused on improving the security, effectiveness, and efficiency of the movement of war materiel
- Funded by the Commonwealth of Pennsylvania, DOD, DHS, and DOT
- DRMEC's Mission:
 - Facilitate communications, collaboration, and coordination among stakeholders
 - Develop and deploy RAPID Center along with supporting automation to facilitate a high-speed, secure (fort-to-port) logistics movement reporting and security coordination system for military and commercial users
 - Support DoD deployments, redeployments, and sustainment operations with RAPID Center
 - Use the Port of Philadelphia as the model for the development of RAPID Center and the supporting automation

IDA's TASKING

B. IDA TASKING

In 2003, the Maritime Administration (MARAD) of the Department of Transportation tasked IDA to initiate an effort to help identify approaches to improve the safety and accountability of war materiel moving between the U.S. Army's forts and the ships at the port of Philadelphia. A focus of this effort was to help DRMEC define the critical elements of a center, called RAPID Center, to coordinate these activities. In 2004, DRMEC tasked IDA to initiate the design and development of an online, wide area network system to enable RAPID Center to send

alerts to the large number of organizations involved in the movement of war materiel, the stakeholders. The alerts are intended to inform the stakeholders of incidences, or the potential occurrence of incidences, that might affect movement of the materiel. In 2005, this tasking was increased to include the design, development, and demonstration of a pilot version of an online system to support the tracking of individual pieces of cargo, to provide a common operational picture to all stakeholders, and to provide a means of alerting the stakeholders. Tasking to identify advanced features for the system was also included.

IDA's TASKING

FY 2003 – MARAD tasks IDA to identify approaches to improve the safety and accountability in the movement of war materiel.

FY 2004 – DRMEC tasks IDA to initiate the design and development of an alert system to support the movement of war materiel.

FY 2005 – DRMEC expands the tasking to include the conception, design, development, testing, and demonstration of an initial pilot system to:

- Automate the process of coordinating and tracking the movement of war materiel between the port of Philadelphia and the U.S. forts sending or receiving the materiel
- Provide a Common Operating Picture to selected organizations
- Provide improved tracking of the shipments
- Provide near real-time alert capability throughout operating region – Wisconsin to New York to Georgia
- Provide information distribution capability

OVERVIEW OF INITIAL DESIGN

C. INITIAL DESIGN

RAPID System is the information hub for RAPID Center connecting users to RAPID Center's information by way of a secure website. On command from RAPID Center, it sends out alerts to inform users of critical information and maintains an information interface to the U.S. Army's Battle Command Sustainment Support System (BCS3) so that participants can use BCS3 to display location, status, and other related information on materiel in transit.

RAPID System, which is based on IDA's IDSS,¹ processes textual and numerical information as well as related graphs and charts and then makes these products accessible to users. In addition, RAPID System provides the information processing backbone for RAPID alerts that go out via cell phone and email to field personnel to provide timely notification of significant events.

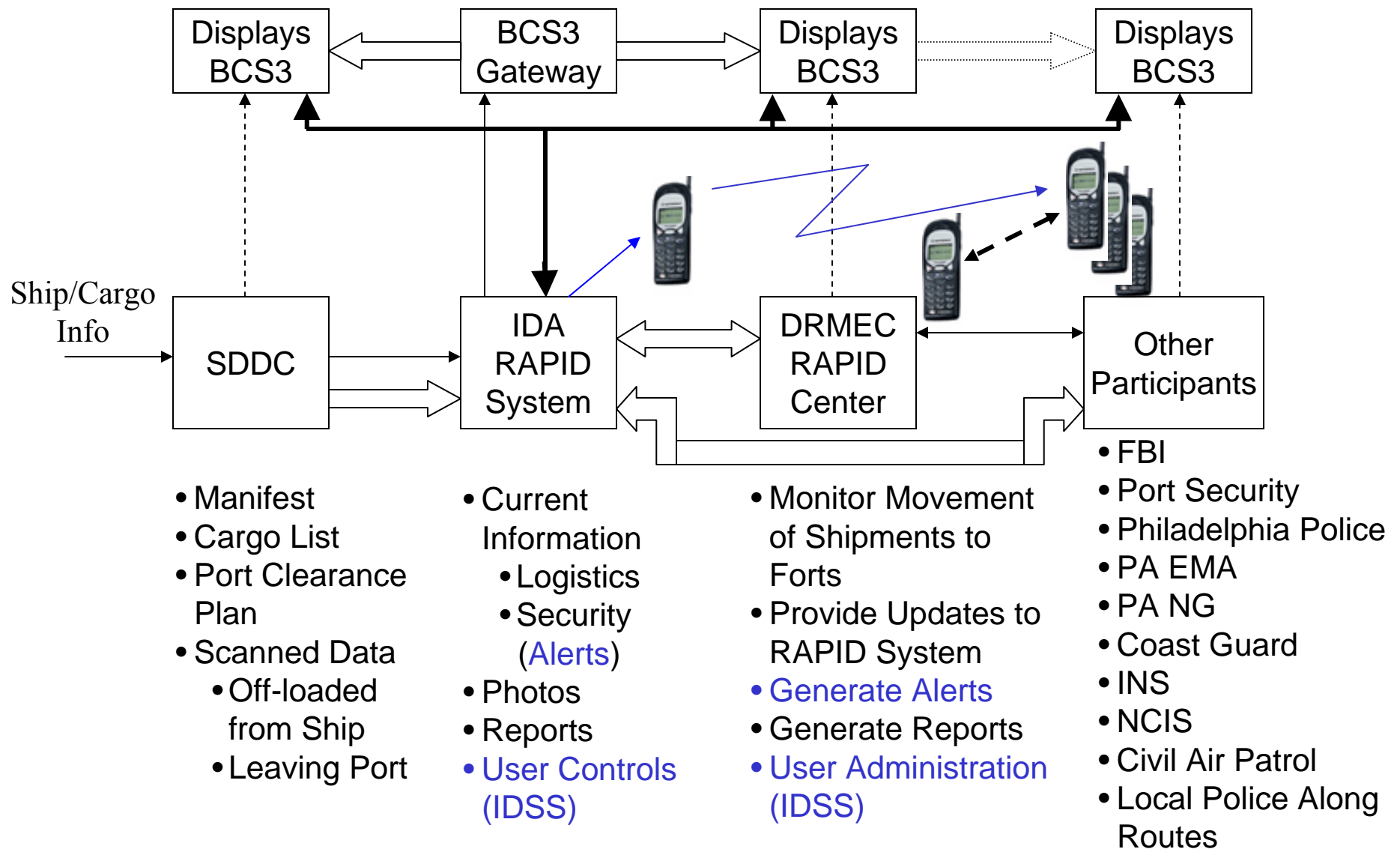
The figure illustrates the RAPID System and DRMEC's RAPID Center as they were used in support of the movement of military equipment through the port of Philadelphia. In the first demonstration the system supported the redeployment of equipment from overseas to 16 destinations, which included depots and home stations of the units that "own" the equipment.

In the second demonstration, it supported the deployment of the 10th Mountain Division from Fort Drum along with the movement of additional cargo from several other forts.

For a redeployment, the essential information that starts the process is the manifest of the ship's cargo that is maintained in the Worldwide Port System (WPS) by the SDDC. For a deployment, it is the cargo list. Some of this information goes into the BCS3 via a national server. For DRMEC's purposes, however, it is sent to RAPID System where it is processed and made available as outlined above. The pictures of cell phones illustrate that RAPID System contains the software for generating alerts and maintains records such as distribution lists for various types of alerts that the DRMEC RAPID Center would need to send out. Items in blue are functions that were in the original tasking for initiating the development of the RAPID Alert System. Items in black were added as a result of the expanded system objectives and are explained in more detail later in this section.

¹ See Appendix B for more detail on IDSS.

OVERVIEW OF INITIAL DESIGN



SUMMARY OF IDA'S INITIAL DEVELOPMENT EFFORT

The primary focal points of IDA's initial development effort were the establishment of the RAPID System website, the design and development of the priority software modules for RAPID System, the hosting of the BCS3 Gateway, and the interface between RAPID System and the BCS3.

Three modules were included in this initial effort; logistics, security, and reports. A fourth module, imagery, was incorporated, but it was not used in the initial effort. The logistics module contains the list of cargo, called the cargo list, to be moved between the forts and the ship. It differs from the cargo manifest in that it contains information on where each item is located (e.g., on the ship, at the port, between the fort and the port) and how it is being moved (e.g., truck, train, military convoy). Each item of cargo contains an ID tag, which is scanned each time it is moved (e.g., taken off the ship or placed on a truck). RAPID System contains an automated means of processing this scanned information to keep the cargo list updated.

The security module contains the capability to send alerts to users who have need for specific information. An example would be a terrorist attack that could affect cargo movement. The initial effort provided two communications means for sending out alerts: text messages sent to mobile phones and email. RAPID System User Information pages are used to specify user mobile phone numbers and service providers, email addresses, and the user preferences for

receiving the messages. If necessary, the RAPID Center sender can modify the preference. For most mobile phones, the text messages were sent using the GSM short message service (SMS). Messages were sent to the NEXTEL mobile phones using the NEXTEL paging service. RAPID System collects and maintains data on the status of the transmission to each wireless device including date and time sent from RAPID System, sent by the service provider to the phone, and read by the recipient.

The reports module provides the capability for selected users at RAPID Center to upload summary reports of logistics and security activities. These summaries can be viewed by all users of RAPID System.

The interface between RAPID System and BCS3 (shown in BOLD on previous page) allows BCS3 users to obtain selected information directly from RAPID System. When a BCS3 user clicks on a 'hot spot' on the BCS3 screen, a process containing a specific URL is started. The URL is used to activate a process in RAPID System that provides the BCS3 workstation with the desired data which it then displays for the user. This process ensures that the user always sees current information. An example of a 'hot spot' would be the location of a fort; data desired would be the cargo being transferred and the status of each item of that cargo.

SUMMARY OF IDA'S INITIAL DEVELOPMENT EFFORT

- **Developed Logistics Module**
 - Automated inputting/updating of:
 - Manifest
 - Cargo list
 - Scanner fileswith discrepancy reports
 - Cargo list – provided:
 - View by fort
 - Indexing on selected columns
 - Tie to manifest
 - Capability to manually update
- **Developed Reports Module**
 - Provided picture/graph capability
 - Provided report upload capability from RAPID Center
- **Developed Security Module**
 - Provided capability to:
 - Send alerts to mobile phones
 - View alert details from PCs or phones
 - Add modify, delete and cancel
- **Hosted BCS3 Gateway**
 - Interfaced to RAPID System
 - Generated hotspots for forts
 - Tied hotspots to fort's data
 - Provided capability for RAPID center to display alert symbol at specified position

TIMELINE OF FIRST DEMONSTRATION

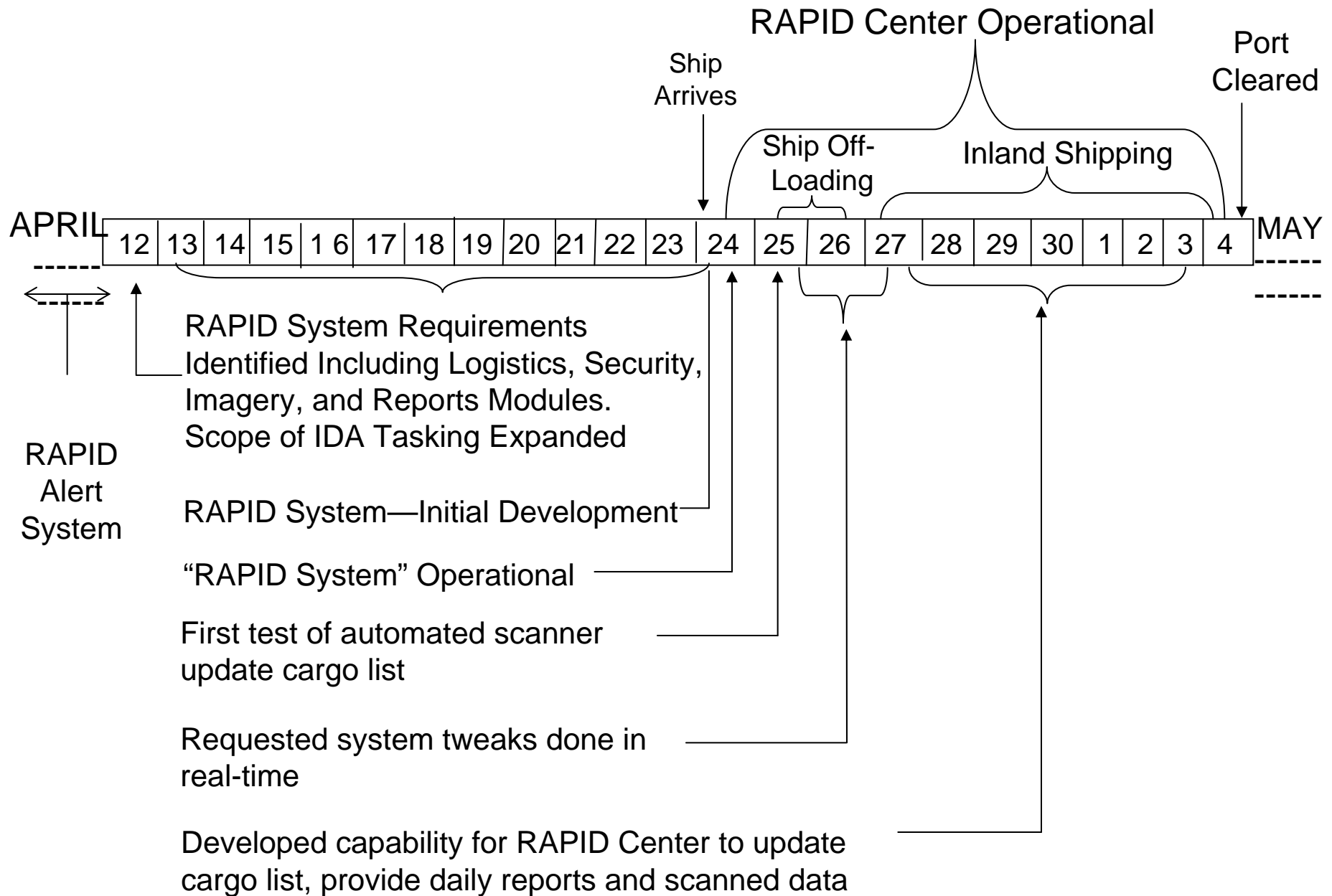
D. FIRST DEMONSTRATION

This chart shows the timeline for the design, development, and first demonstration of RAPID System. Prior to the DRMEC/Government/IDA meeting, which started on 12 April, the IDA effort had been focused on the design and development of the RAPID alert system—a system to allow RAPID Center to quickly send alerts to responders and stakeholders. During the meeting it was recognized that a more comprehensive system, called RAPID System, was required. Specifically, logistics, reports, and imagery modules needed to be added and the alert system needed to be expanded into a more comprehensive security module.

Using the IDSS platform (see Appendix B) along with the benefit of years of experience in building similar

systems, IDA was able to have the initial elements of RAPID System operational as the ship with its cargo of war materiel arrived at the port of Philadelphia, and RAPID Center became operational on 24 September. As RAPID Center began its initial use of RAPID System, the desirability of additional features began to come to light along with ideas on how to improve existing ones. Examples include using the bar code scans from each piece of cargo as it was offloaded from the ship and as it left the port to update the cargo list in RAPID System and publishing daily reports on the logistics and security activities. Initially, IDA personnel had to manually input data into the system, however, the system was soon upgraded to allow those in RAPID Center to input the data in an automated fashion.

TIMELINE OF FIRST DEMONSTRATION



PHOTOS FROM FIRST DEMONSTRATION

The next three photographs illustrate the first demonstration. The first picture shows an overview of the Packer Avenue Marine Terminal where the ship docked. It also shows the Pier 98 Annex where materiel taken off the ship was located before it was transported to forts and railroad lines available in the area. To the left of the road,

directly under the overpass, is the three-wide trailer that housed RAPID Center during this operation. RAPID Center is expected to move to the location shown in the picture in the near term.

Appendix C contains additional pictures from the first demonstration.



PHOTOS FROM THE FIRST DEMONSTRATION (Continued)

This picture was taken in RAPID Center. It shows two of the displays supported by RAPID System. The login screen for RAPID System is on the left. The BCS3 display is on the right and shows a map, which is enlarged on the following page.

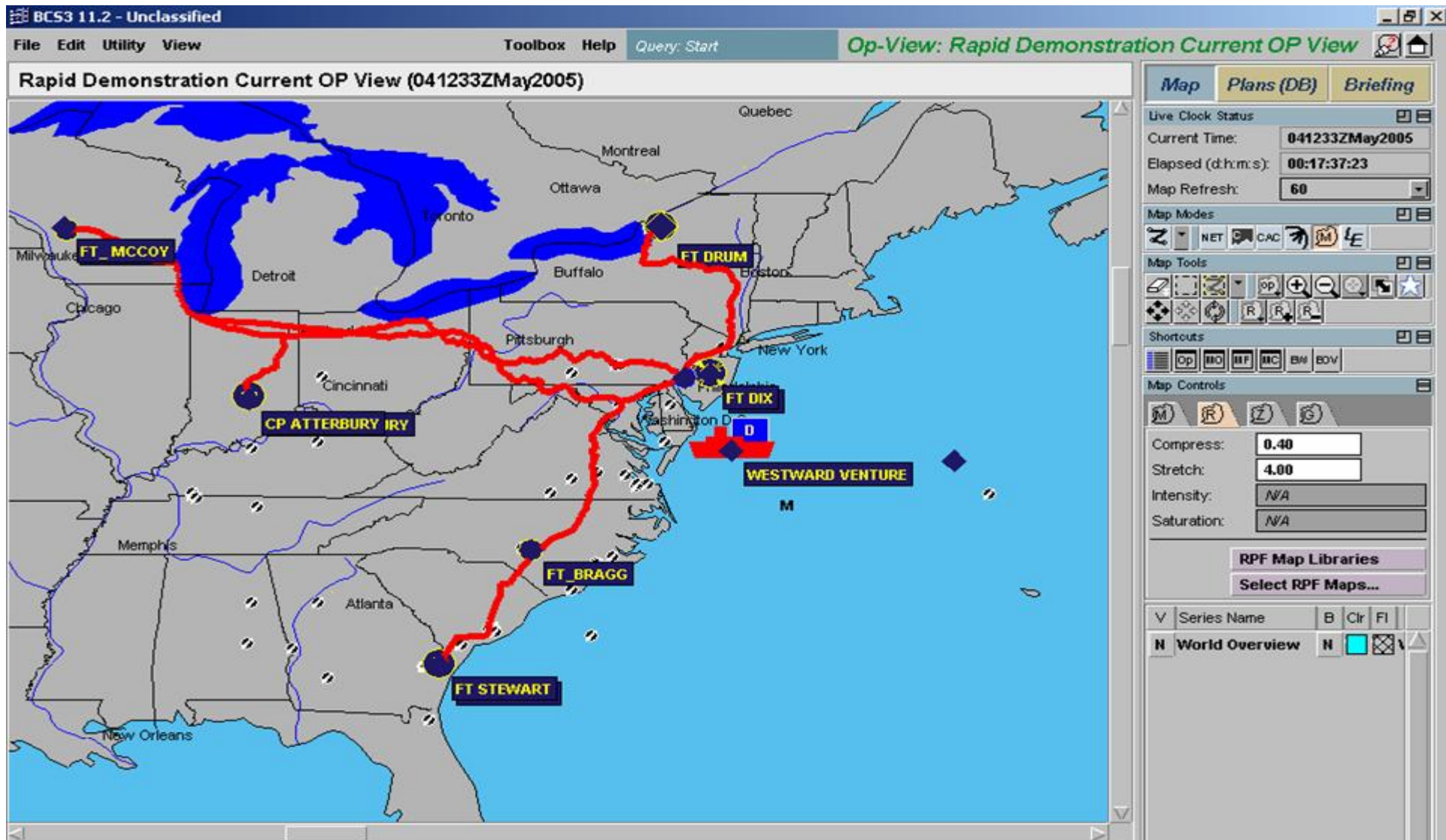


PHOTOS FROM THE FIRST DEMONSTRATION (continued)

This BCS3 screen contains a map showing the location of the ship, Westward Venture, at the port of Philadelphia, six of the forts to which the materiel from the ship is to be delivered, and the approximate location of the railroad tracks that connect the forts to the port.

Clicking the mouse on one of the forts shown brings up a list of the cargo destined for that fort along with the status

of each item. The cargo data reside in RAPID System, which configures it for display on BCS3 in response to the mouse click. As a result, the BCS3 operators always receive the latest data available regardless of their physical location.



**Battle Command Sustainment Support System
Screen for RAPID Center Demonstration**

EXAMPLE OF THE CARGO LIST

This is an example of a cargo list as displayed by RAPID System's logistics module. For materiel being returned to the United States, the cargo list is derived from the ship's manifest. Its purpose is to provide information on each item removed from the ship. Information includes the item's ultimate destination, the transportation mode to be used to deliver the item, and the item's current status. Status includes codes for 'still on the ship,' 'at the port,' 'loaded on the transportation vehicle,' 'left the port,' and 'arrived at the destination.'

The graphic shows a portion of page one of the list of cargo being sent to Camp Atterbury. Items shown on the cargo list include:

- ULN – Unit Line Number
- Consignee – Organization to which item is being shipped
- Mdl Num – Model number (containers have none)
- Desc – Description of item
- Bmpr Num – Unit assigned number for vehicle
- TCN – Transportation Control Number
- Comdty Spec Hndlg – Code to indicate whether or not item requires special handling
- Length, Width, Height & Weight – Item characteristics

Clicking on the blue underlined header of a column will put the cargo list in order by the information in that column—highest to lowest, most recent to previous dates.

Cargo list BCS3 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address https://www.idss.ida.org/rapidsystem/ids/CargoList/CargoList_view_bcs3.prg?bcs3=YES&sel_dest=CP%20ATTERBURY Go Links

Goto Page: [Next](#) 1 2 3 4

CP ATTERBURY: Cargo List Page 1 of 4

UIC	ULN	Noun Name	Amt	Consignee	Mdl Num	Desc.	Bmpr Num	TCN	Comdty Spec Hndlg	RFID	Serial Num	Length	Width	Height	Weight	Location	Mode
WPDKB0		0216 EN BN CO B	1	WPDKB0	M51A2	TRUCK DUMP 5-TON B-93		AWPDKB0\$0D90360XX	882ZZ		C13310103	266	128	112	22244	R	IT
WPPTD0	TAQD 01	0152 IN BN 01 CO D	1	WPPTD0	M998A1	TRK UTIL CRG/TRP	D-02	AWPPTD0\$0D00220XX	867Z9		157642	191	86	82	5380	R	T
WPPTD0	TAQD 01	0152 IN BN 01 CO D	1	WPPTD0	M1038	TRK UTIL CGO/TRP	HQ-26	AWPPTD0\$0D00520XX	867Z9		115877	191	86	82	5200	R	IT
WPPTD0	TAQD 01	0152 IN BN 01 CO D	1	WPPTD0	M1038	TRK UTIL/TRP CARR D-03		AWPPTD0\$0D00160XX	867Z9		117567	191	86	82	5200	R	T
WPPTD0	TAQD 01	0152 IN BN 01 CO D	1	WPPTD0	M1038	TRK UTIL/TRP CARR D-05		AWPPTD0\$0D00190XX	867Z9		115954	188	86	82	5200	R	IT
WPPTD0	TAQD 01	0152 IN BN 01 CO D	1	WPPTD0	M1038	TRK UTIL/TRP CARR D-07		AWPPTD0\$0D00320XX	867Z9		115860	191	86	82	5200	R	IT
WPPTD0	TAQD 01	0152 IN BN 01 CO D	1	WPPTD0	M1038	TRK UTIL/TRP CARR D-09		AWPPTD0\$0D00180XX	867Z9		115866	191	86	82	5200	R	IT
WPPTD0	TAQD 01	0152 IN BN 01 CO D	1	WPPTD0	M1038	TRK UTIL/TRP CARR D-11		AWPPTD0\$0D00170XX	867Z9		117561	191	86	82	5200	R	T
WPPTD0	TAQD 01	0152 IN BN 01 CO D	1	WPPTD0	M966	TRK UTIL TOW CAR D-14		AWPPTD0\$0D00010XX	867Z9		20879	188	86	78	7195	R	IT
WPPTD0	TAQD 01	0152 IN BN 01 CO D	1	WPPTD0	M966	TRK UTIL TOW CAR D-16		AWPPTD0\$0D00020XX	867Z9		20849	191	86	87	7195	R	T
WPPTD0	TAQD 01	0152 IN BN 01 CO D	1	WPPTD0	M966	TRK UTIL TOW CAR D-18		AWPPTD0\$0D00080XX	867Z9		20891	188	86	82	7195	R	IT

Done

Hiding your inactive notification icons... To see the hidden icons, click this button.

start BCS3 11.2 - Unclassified C:\Documents and Se... Cargo list BCS3 - Mic... 3:08 PM

EXAMPLE OF A RAPID SYSTEM ALERT

This screen shows an example of an alert issued by RAPID Center using the RAPID System security module during the first demonstration of the system. These alerts are used to keep stakeholder organizations, including first responders, aware of important events or milestones.

Most stakeholders receive notification of an alert by way of their mobile phones; email notification was added after the first demonstration. The notification contains the alert number along with the title. Because of the potential sensitivity of the information contained in the text of the alert, users need to connect to the RAPID System website by way of a secure link in order to access that information. One

can connect to the website with one's mobile phone and other mobile devices as well as a PC. Alerts can also have attachments containing text, pictures, or maps. These, too, can be displayed on mobile phones and other mobile devices as well as PCs.

RAPID System maintains information on when alerts are sent from RAPID Center, when they are delivered to the Cingular network, when the network indicates they are delivered to the wireless phones, and when the user first reads them. It also indicates if there was difficulty in sending the alert to any users.

Alert Information - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites Media Print Mail News RSS Feeds

Address https://www.idss.ida.org/rapidsystem/alert/disp_alert?alertnum=120 Go Links

Title: Security Alert - Train Movement Destined for Ft. McCoy, WI

Level: 1

Added: 05/02/2005 08:53:35 AM

Approved: 05/02/2005 08:54:18 AM by Mr. Joseph Alkus

Expires: 05/09/2005 12:00:00 AM

Alert - For Official Use Only –

Text:

RAPID CENTER ALERT

RAPID Center reports that at 8:45 AM, today (May 2) the train destined for Fort McCoy, Wisconsin is preparing to depart the Packer Avenue Marine Terminal. The train has 10 rail cars with 10 pieces of cargo loaded. Recipients are requested to report any suspicious behaviors, activities, vehicles, packages, etc., surrounding port, rail, and appropriate transportation critical infrastructures to Philadelphia Police and RAPID Center that may affect this movement.

RAPID Center requests immediate notification of manmade, natural, special events, and/or accidents that may impact and/or impede the flow of these military equipment movements regarding rail, road, bridge and port infrastructures.

RAPID Center is operational between the hours of 8:00 AM to 6:00 PM and can be reached at 215-551-2932 or 215-551-2771 and FAX Number 215-551-2985. After hours the RAPID Center Duty Officer can be reached at 215-892-4034 or Nextel Direct Connect 168*93587*4

RAPID Center will issue a Daily Summary Report at 6:00 PM, which will be available on RAPID System's Secure Web Site at

<https://www.idss.ida.org/rapidsystem/login>

RAPID Center is a neutral secure information sharing facility demonstrating new business processes and technologies in support of DOD deployment and redeployment movements through the Strategic Port of Philadelphia. RAPID Center is part of RAPID System—an advanced distribution solution for military and commercial markets. RAPID System partners

Done Internet

start Inbox - Microsoft Out... CNN.com - Microsoft ... Alert Information - Mi... Microsoft PowerPoint ... 11:20 AM

EXAMPLES OF CARGO AND SECURITY STATUS REPORTS

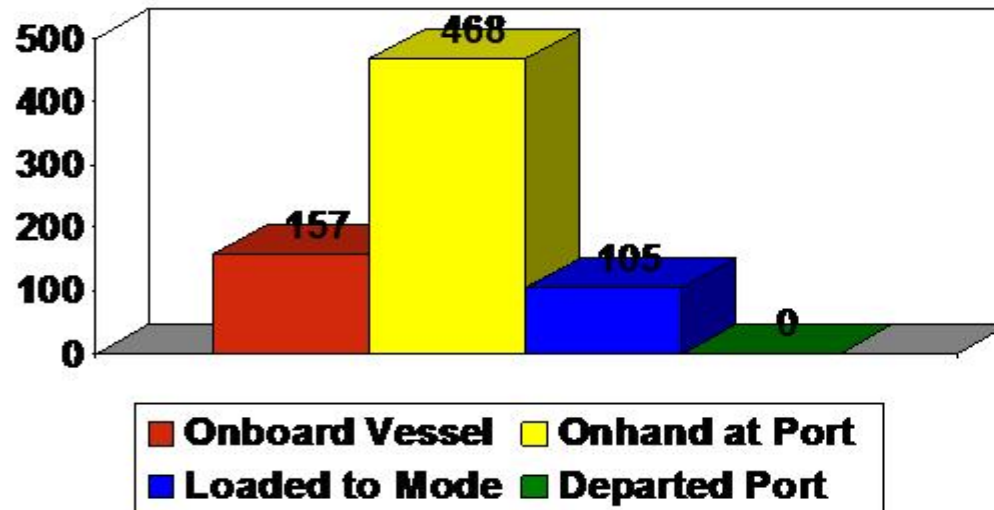
This chart shows the cargo status as of 27 April at 0800 hours. The diagram in the upper left-hand corner shows the amount of cargo still on the ship, the amount stored at the port, the amount loaded on vehicles that will transport the items to the forts and the number of items that have departed the port. Pictures show events at the port.

Cargo Status

Discharge at Port of Philadelphia

As of 27 April 2005 0800 hours EDT

Westward Venture Voyage M4547



- Cargo Discharge Continues
- Truck Departures Begin
- Rail Cars Continue to Load



EXAMPLES OF CARGO AND SECURITY STATUS REPORTS (continued)

This is an example of a security report. The text in the center provides a summary of the security status operations as of 1800 hours on 29 April. The pictures show recent events at the port.

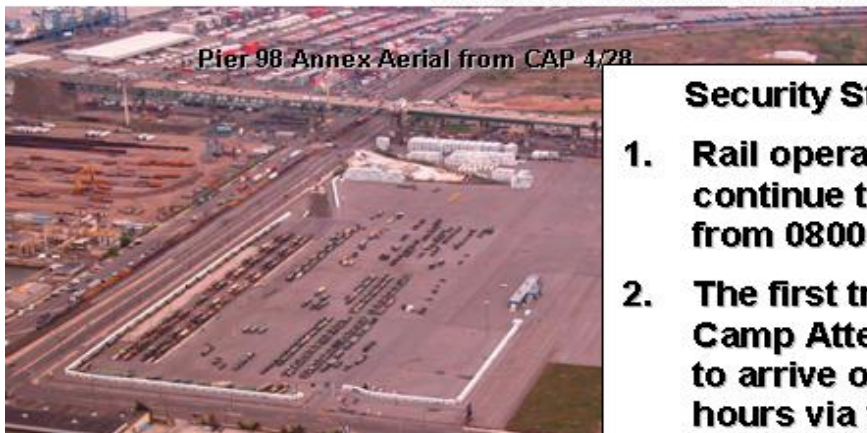


RAPID Center

Regional Agile Port Intermodal Distribution System Center

Security Report

As of 29 April 2005 1800 hours EDT



Pier 98 Annex Aerial from CAP 4/28

Security Status Report – 1800 hours

1. Rail operations are scheduled to continue throughout the weekend, from 0800 hours to 1700 hours.
2. The first train which departed for Camp Atterbury, Indiana is expected to arrive on Sunday 1 May at 2100 hours via the Norfolk Southern Rail Lines. This train contained approximately 30 rail cargos.
3. The second train destined for Camp Atterbury is expected to depart the Pier 98 Annex today at 2100 hours.
4. No truck departures are scheduled for the weekend.

To Contact RAPID Center Security Duty Officer Call

215-892-4034

Nextel Direct Connect 168*93587*4



Tanker Trucks Loading on Rail Cars



Tanker Trucks Loading on Rail Cars



Tanker Trucks Loading on Rail Cars

SUMMARY OF ACTIVITY DURING THE FIRST DEMONSTRATION

The first demonstration of RAPID System spanned 11 days. From the ship, 733 items were off-loaded and transferred to 16 different locations—178 by rail car and 205 by truck. All items taken off the ship were delivered to their intended forts.

Although many security alerts were sent by RAPID Center, using RAPID System, one of particular interest involved a bomb found on a railroad track.

Even though the bomb did not endanger any of the materiel being moved, it did provide an opportunity to demonstrate the speed with which RAPID Center sends an alert.

SUMMARY OF ACTIVITY DURING THE FIRST DEMONSTRATION

- RAPID System performed as designed
 - An 11-day operation
- Logistics Module provided continuous status of cargo
 - 733 items transferred
 - 178 rail cars to 4 locations
 - 205 trucks to 16 locations
- Significant incident
 - Bomb found on railroad track
 - Reported via RAPID security module

SECOND DEMONSTRATION

E. SECOND DEMONSTRATION

The second use of RAPID System was in support of the deployment of the 10th Mountain Division from Fort Drum through the port of Philadelphia as it moved to its new location overseas. Additional cargo for the ship came from Camp Atterbury, Camp Shelby, and Fort Dix.

For this operation, RAPID Center and RAPID System became operational on 27 June, 2005. Most of the cargo from Fort Drum was transported by train. The first train

left Fort Drum on 29 June and arrived at the port of Philadelphia on 30 June. The second train left Fort Drum on 7 July and arrived at the port on 9 July. Most of the other cargo from Fort Drum, as well as the other locations, was moved by truck and arrived between 27 June and 9 July. The ship was loaded between 10 and 12 July. Although it was scheduled to sail on 12 July, an engine problem delayed that until the 13th.

RAPID Center and RAPID System returned to standby status on 12 July.

SECOND DEMONSTRATION

TIMELINE OF EVENTS DURING SECOND DEMONSTRATION

This chart shows the timeline of the events of the second demonstration in 2005 and some events that necessitated changes to RAPID System.

- 14 June—Received test WPS update file in a new format.
- 29 June—Received file format for pseudo-manifest file and first pseudo-manifest. Initiated parsing program for pseudo-manifest file to provide data to support “view manifest” feature on cargo list.
- 01 July—Received a WPS update file, but was not in same format as test, necessitating manual reformatting of file and manual running of update process.
- 05 July—Finished parsing program for the pseudo-manifest file.
 - Received WPS update files in another new format. Found that originating and destination location fields in update files were not valid. Told to use UIC to determine where cargo was coming from. Started database table to link UIC to fort.
- 07 July—WPS file format stabilized, update program modified, and auto-update process started, removing the need to perform manual updates.
- 08 July—WPS file arrived with unknown (to IDA) UICs.
- 09 July—Auto-update program changed to mark unknown UICs as coming from “UNKNOWN” location. Automatic update process was changed to check for updates every 10 instead of 20 minutes.

During two time periods, alerts did not go out in a timely manner to non-Nextel mobile phones:

July 7, from 9:51 AM to 1:50 PM. Alert affected:

#16: Second train departing from Fort Drum, etc.

July 9, from 1:34 PM to 2:20 PM. Alerts affected:

#22: M/V Westward Venture arrives at Packer Ave Marine Terminal, etc.

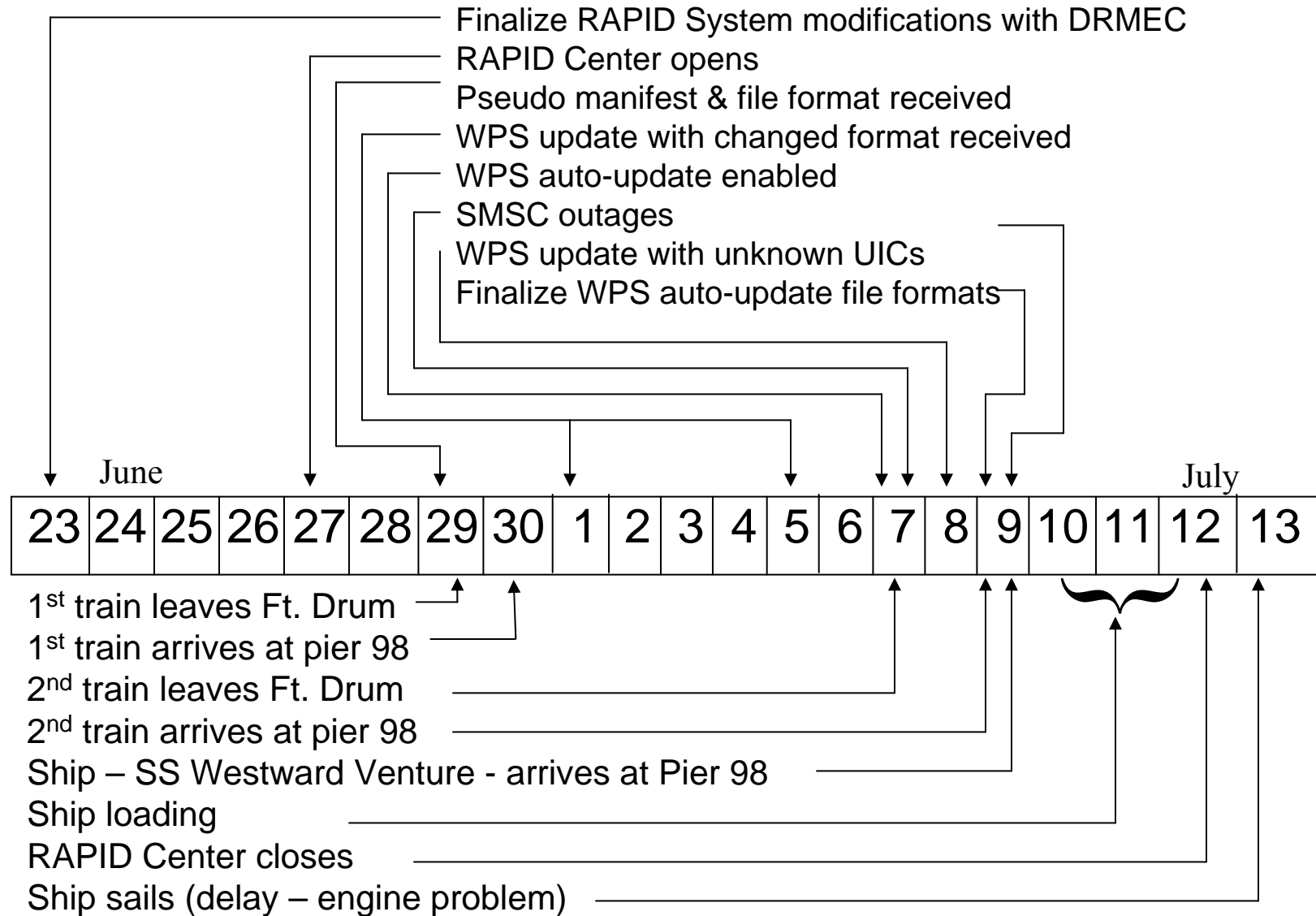
#23: Daily cargo summary and security status reports available, etc.

The outages may have occurred earlier but the system only collects data when it tries to send alerts.

In both cases, the faults were traced to the AT&T Wireless (now Cingular) SMS Centers that the system uses to send SMS messages and were confirmed by phone with Cingular tech support. Also, in both instances, IDA tried to bypass its own equipment and software and send text messages manually over AT&T Wireless handsets. However, the same “message sending failed” error messages were received.

During both outages, IDA sent alerts “by hand” by going to the AT&T Wireless text-messaging website. However, outage discovery and verification along with the manual sending process caused messages to be delayed 30-60 minutes.

TIMELINE OF EVENTS DURING SECOND DEMONSTRATION



EXAMPLE OF THE CARGO LIST

This screen shows part of the cargo list for the second use of RAPID System. While the data fields in the cargo list are essentially the same as those used for the first ship, some modifications were made to make the list more useful and easier to read. Changes included adding lines to separate rows and columns, adding several fields


(columns) namely UN Class and UN Number, rearranging columns, and adding information on Vessel Name (Vessel), temporary voyage number (BVOY), final voyage number (VOY #) and Move Type at the top of the list.

IDS Manager - Mainfest - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address https://www.idss.ida.org/rapidsystem/ids/cargolist/CargoList_view Go Links



RAPID System
Regional Agile Port Intermodal Distribution System

Find TCN Back to Selection Page Goto Page: [Next»](#) 1 2 3 4 5 6 7 8 9 10 11 12

Vessel: WESTWARD VENTURE **As of:** 07/
BVOY: A3402 **POE:** Phil
Voy #: A3402 **POD:** Kur
Move Type: deploy

Cargo List Page 1 of 12

Origin: UIC	TCN	ULN	UNIT	Consignee	Mtl. Num	Desc.	Bmpr/ Container Num	Comdty Spec Hndlg	UN Class	UN Number	Serial Num	Pcs
FT DRUM: WJJVT0	AWJJVT0\$0D00080XX edit cargo : view manifest	T103C		WJJVT0	PU-798	GEN SET DED TRL MTD	H30TG	89229			296	1
FT DRUM: WJJVT0	AWJJVT0\$0D00410XX edit cargo : view manifest	T103C		WJJVT0	M1113	TRK UTIL EXPANDED CA	HHC12	86729				1
FT DRUM: WJJVT0	AWJJVT0\$0D00420XX edit cargo : view manifest	T103C		WJJVT0	PU-798	GEN SET DED TRL MTD	HHC 12T	89229				1
FT DRUM: WJJVT0	AWJJVT0\$0D00430XX edit cargo : view manifest	T103C		WJJVT0	PU-798	GEN SET DED TRL MTD	H-97TG	89229				1
FT DRUM: WJJVT0	AWJJVT0\$0D00550XX edit cargo : view manifest	T103C		WJJVT0	M149A2	TRLR TK WTR 400 GAL	HHC-2T	89229			04G4-120	1
FT DRUM: WJJVT0	AWJJVT0\$0D00560XX edit cargo : view manifest	T103C		WJJVT0	M149A2	TRLR TK WTR 400 GAL	HHC-3T	89229			523	1

Internet

EXAMPLE OF A RAPID SYSTEM ALERT

This screen represents an example of an alert issued by RAPID Center during the second use of RAPID System. The format is essentially the same as that used in the first demonstration.

Alert Information - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites Media

Address https://www.idss.ida.org/rapidsystem/alert/disp_alert?alertnum=4 Go Links

Title: RAPID CENTER ALERT # 3 First Fort Drum Train Departs for Philadelphia
<https://www.idss.ida.org/rapidsystem/1>

Level: 1

Added: 06/30/2005 06:50:06 AM

Approved: 06/30/2005 06:52:12 AM by Mr. Joseph Allkus

Expires: 07/07/2005 12:00:00 AM

Alert - For Official Use Only –

Text:

RAPID CENTER ALERT # 3 First Fort Drum Train Departs for Philadelphia

<https://www.idss.ida.org/rapidsystem/login>

RAPID Center reports that at approximately 0500 hours EDT, the first train departed from Fort Drum, New York destined for the Port of Philadelphia. The train contains 63 rail cars and 351 pieces of military cargo. The projected rail route for this train is on CSX rail lines from Fort Drum, to Watertown, NY; Syracuse, NY; Selkirk, NY; North Junction, NY, Kearny, NJ; Princeton Junction; West Trenton, NY into Pennsylvania and onto the Greenwich Terminal near the Port of Philadelphia. The approximate travel time from Fort Drum to Greenwich Terminal is between 18 and 24 hours. The train is equipped with a GPS tracking device that will be monitored by the Movement Tracking System and viewable on the Army's Battle Command Sustainment Support System (BCS3). RAPID Center will provide periodic reports on the train's progress under separate alerts along with mapping data.

RAPID Center requests immediate notification of manmade, natural, special events, and/or accidents that may affect and/or impede the flow of this military equipment movement over road, rail, bridge, and port infrastructures.

RAPID Center is operational between the hours of 8:00 AM to 6:00 PM and can be reached at 215-551-2932 or 2771 and FAX Number 215-551-2985. After hours the RAPID Center Duty Officer can be reached at 215-

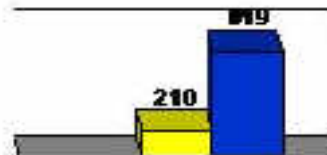
EXAMPLES OF THE CARGO AND SECURITY STATUS REPORTS

The next two charts show examples of reports that were made available on RAPID System during the second use of the system. The first chart show the cargo status as of 12 July at 1600 hours. The diagram in the upper left-hand corner shows the cargo status. That is, the amount of cargo

expected to arrive from the forts and be loaded on the ship, the amount that has arrived at the port, and the amount currently loaded on the ship. The photos are of events at the port.

**June/July Cargo Deployment
Cargo Activity**

■ Expected Pieces
■ Arrived at Port
■ Loaded to Mode



**Cargo Status
Port of Philadelphia
As of July 12, 2005 1600 hours EDT**

1. Vessel loading operation are expected to be concluded by 1800 today.
2. The cargo (72 pieces) expected from Camp Shelby have been cancelled.
3. Total piece count for this operation is 1029 pieces.

SECURITY STATUS REPORT

This is an example of a Security Report. Text in the center provides a summary of the security status operations as of 1600 hours on 12 July. The pictures show recent events at the port.

Security Status Report

July 12, 2005

1600 hours EDT



RAPID Center

Regional Agile Port Intermodal Distribution System Center

1. The military equipment uploading to SS Westward Venture continues with an anticipated completion during the evening hours of 7/12/05.
2. From 1000 hours to 1230 hours today, RAPID Center participated in an information sharing demonstration with representatives of Office of Secretary of Defense – Homeland Defense, Critical Infrastructure Program (CIP) Architecture, Washington, D.C. (WDC); US Transportation Command (USTRANSCOM) J-5 CIP, Scott Air Force Base, IL; Department of Defense (DOD) Defense Program Office for Mission Assurance, R & D Requirements and Evaluation, and DOD Mission Assurance Support Center, Dahlgren, VA; Association of American Railroads (AAR), WDC and CSX Transportation. DRMEC extends its appreciation to DOD components, CSX and AAR for their outstanding participation.
3. Robert Bouchard representing the US. Maritime Administration (MARAD), Washington, DC visited RAPID Center's Seaport Operation Center. MARAD is supporting the development of RAPID System through a DRMEC/MARAD/SDDC Cooperative agreement.
4. Based on the completion of the upload to vessel, DRMEC's Seaport Operation Center, RAPID Center will close effective 7/12/05 at 1800 hours. RAPID Center Duty Officer can continue to be reached at 215-892-4034 after hours. During normal business hours, DRMEC senior team can be reached for questions regarding RAPID Center at 215-633-7312



Aerial Photo Courtesy of PA Civil Air Patrol



SUMMARY OF ACTIVITY DURING THE SECOND DEMONSTRATION

During the second use of RAPID System, 1,029 items were transferred from the forts to the port of Philadelphia and loaded onto the ship.

Although many security alerts were sent by RAPID Center, using RAPID System, two were of particular interest. Alert number 8 notified users that a small plane that crashed near the route of a train carrying war materiel was not associated with the Civil Air Patrol (CAP) aerial activity observing the train's movement. Alert number 16, sent early on 7 July, noted the London bombings and reminded users to maintain heightened awareness for indicators associated with possible terrorist activity.

When the bombings occurred in London on 7 July, the second train was still in a secure area at Fort Drum although it was nearly ready to depart. Upon hearing of

the bombings, RAPID Center notified organizations responsible for the cargo's movement and aided in their collaboration to ensure that those terrorist attacks would not be followed by other actions that would endanger the train. This effort along with other observations made during the demonstration provided an indication that a collaboration capability should be added to RAPID System.

After the demonstration was completed, SDDC indicated that simultaneous materiel movements may be scheduled for the fall of 2005 potentially at the ports of Philadelphia and Savannah. This would necessitate RAPID Center and RAPID System to support two operations at once.

SUMMARY OF ACTIVITY DURING THE SECOND DEMONSTRATION

- RAPID System performed as designed
 - A 16-day operation
- Logistics module provided continuous status of cargo
 - 1,029 items transferred
 - Two trains from Fort Drum
 - Multiple trucks from 3 locations
- Significant Incidents Reported or Coordinated Using the Security module:
 - Plane crash not related to movement of materiel
 - London bombings not indicator of simultaneous attack on U.S. or threat to the train about to leave Fort Drum

POTENTIAL NEXT STEPS

F. POTENTIAL NEXT STEPS

1. First Steps

Next steps currently being considered are shown here. Given that RAPID System is a spiral development effort, the next task is to document and incorporate changes that came to light during the last demonstration. Also, as the number of users continues to expand, it is important to keep the User's Guide updated.

2. Making a Case for Virtual Collaboration

However, the most significant change is the collaboration capability, which we will discuss now, beginning with the current role RAPID Center plays in

moving war materiel. We will then review some events that occurred during the initial two demonstrations to show that RAPID Center is in a unique position to provide real-time aid to responders during a crisis.

One way this can be done is by expanding RAPID System to include a virtual collaboration capability.

The remainder of this report describes the opportunity RAPID Center has to provide its stakeholders with the capability to quickly coordinate their efforts in response to an unforeseen event that requires a coordinated response. It also describes the current efforts to bring about that capability, provides some examples, and indicates potential next steps.

NEXT STEPS

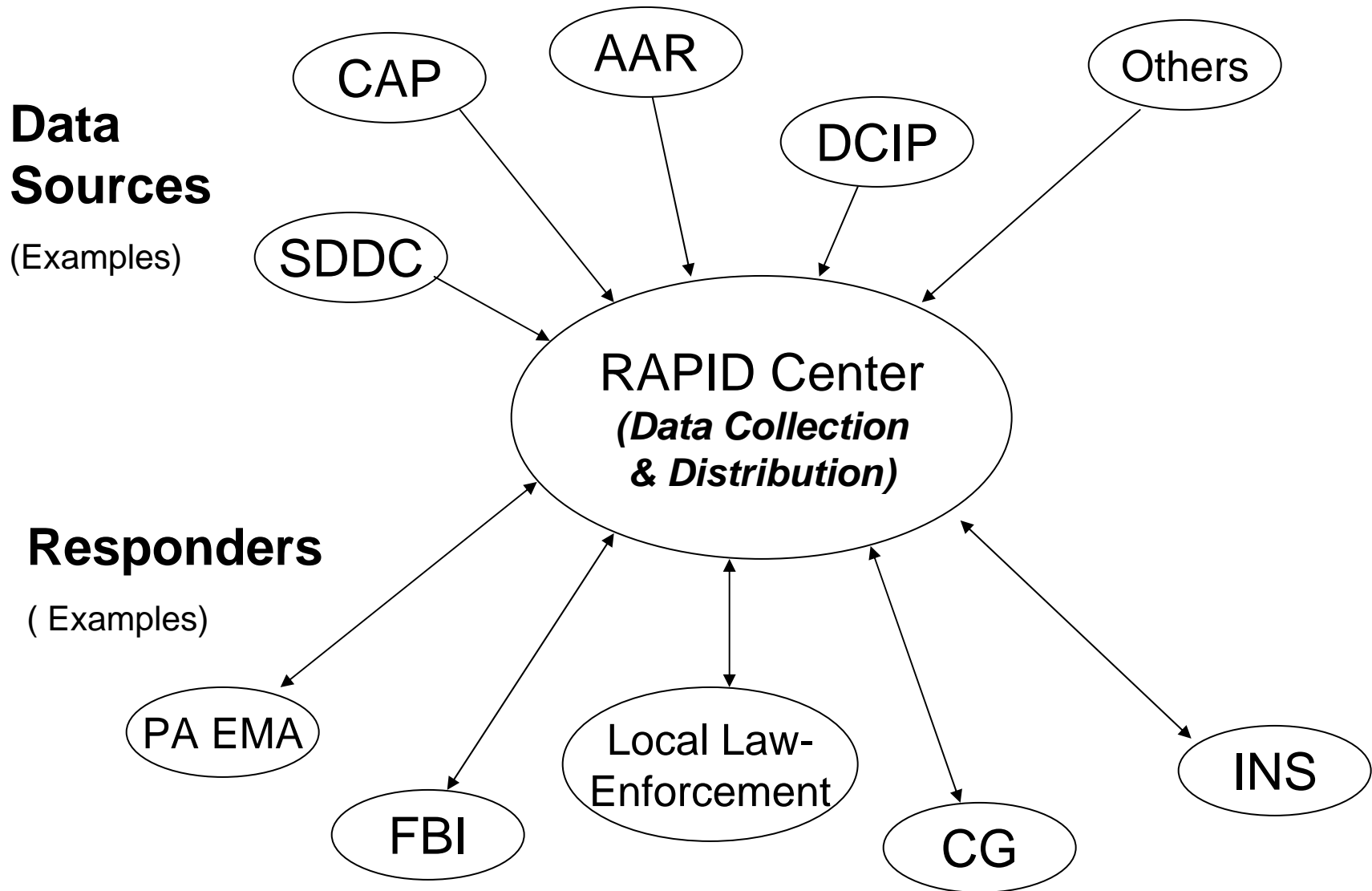
- Define RAPID System modifications desired for the next demonstration
- Documentation – Update User's Guide & System Manuals
- Identify collaboration capability desired in RAPID System and develop plan for incorporating it into the system along with a concept of operations

THE CURRENT SITUATION

In the current situation, RAPID Center collects data from many sources, arranges it into preplanned formats, and provides it in meaningful reports for users. When appropriate, RAPID Center also provides alerts to call user attention to specific events—past or expected. Thus, RAPID Center provides a means to keep users informed. However, in the event the data provided calls attention to a

disaster or potential disaster to which some users must respond, currently no means exist within RAPID Center so users can collaborate on necessary actions beyond participating in a conference call. Since the cargo is generally transported over a number of States, this could lead to missed opportunities to avoid preventable disasters and less than optimum relief when disasters do occur.

THE CURRENT SITUATION



SOME RECENT EVENTS

In the initial two RAPID Center/RAPID System demonstrations, several events could have resulted in broader actions. In the first demonstration, a bomb was found on railroad tracks. While the bomb was not in a position to threaten movement of DoD's cargo and RAPID Center sent out an alert to inform stakeholders, a different location could have necessitated collaboration by several agencies.

In the second demonstration, a small plane crashed near the rail route to be used to move DoD cargo. Again, the event was not a threat to the cargo and RAPID Center sent out an alert to inform the stakeholders.

In the early hours following the London Bombings on 7/7/05, there was considerable concern about additional

attacks within the continental United States (CONUS). In the second demo, some of the cargo being moved was loaded on a train at Fort Drum. After the bombings, advisory questions arose about the train's location and movement permitted under DHS' threat advisory. During this period, RAPID Center supported collaboration among the organizations responsible for safely moving the DoD cargo.

All three alerts were quickly handled, but indicate the requirement for and the value of an expanded collaboration capability when events can directly affect cargo movement.

SOME RECENT EVENTS

- Bomb found on railroad tracks – Sent alert
- Small plane crashes near rail route – Sent alert
- London bombings – Supported ***collaboration*** among responsible parties on movement of train

POTENTIAL OPPORTUNITY

As indicated in the demonstrations, disasters can be caused by terrorists, natural phenomena, or accidents that immobilize a local area. When a disaster does occur, its severity is likely to be measured by the speed with which the responders act and the degree to which they work together. However, disasters do not know municipal boundaries. In fact, terrorists might try to create disasters which cross such boundaries to increase the impact of their acts. In most cases, crossing municipal boundaries means

that the responders do not have a common chief – at least not one who can coordinate activities across boundaries in the short period of time generally available.

Although addressing the overarching command and control issue is beyond the scope of this report, there is an opportunity for RAPID Center to expand its capability to support collaboration among the responders to help facilitate whatever solution is implemented. The next chart shows a first step.

POTENTIAL OPPORTUNITY

- Terrorist, natural phenomena and major local problem all cause disasters
- If a disaster occurs (or might occur) that involves cargo being moved, ***speed*** and ***coordinated efforts*** can minimize the effect (or even prevent the occurrence)
- But, what information sources will responders turn to and how can they use them to coordinate their response?
- Potential for RAPID Center to provide responders with collaboration support

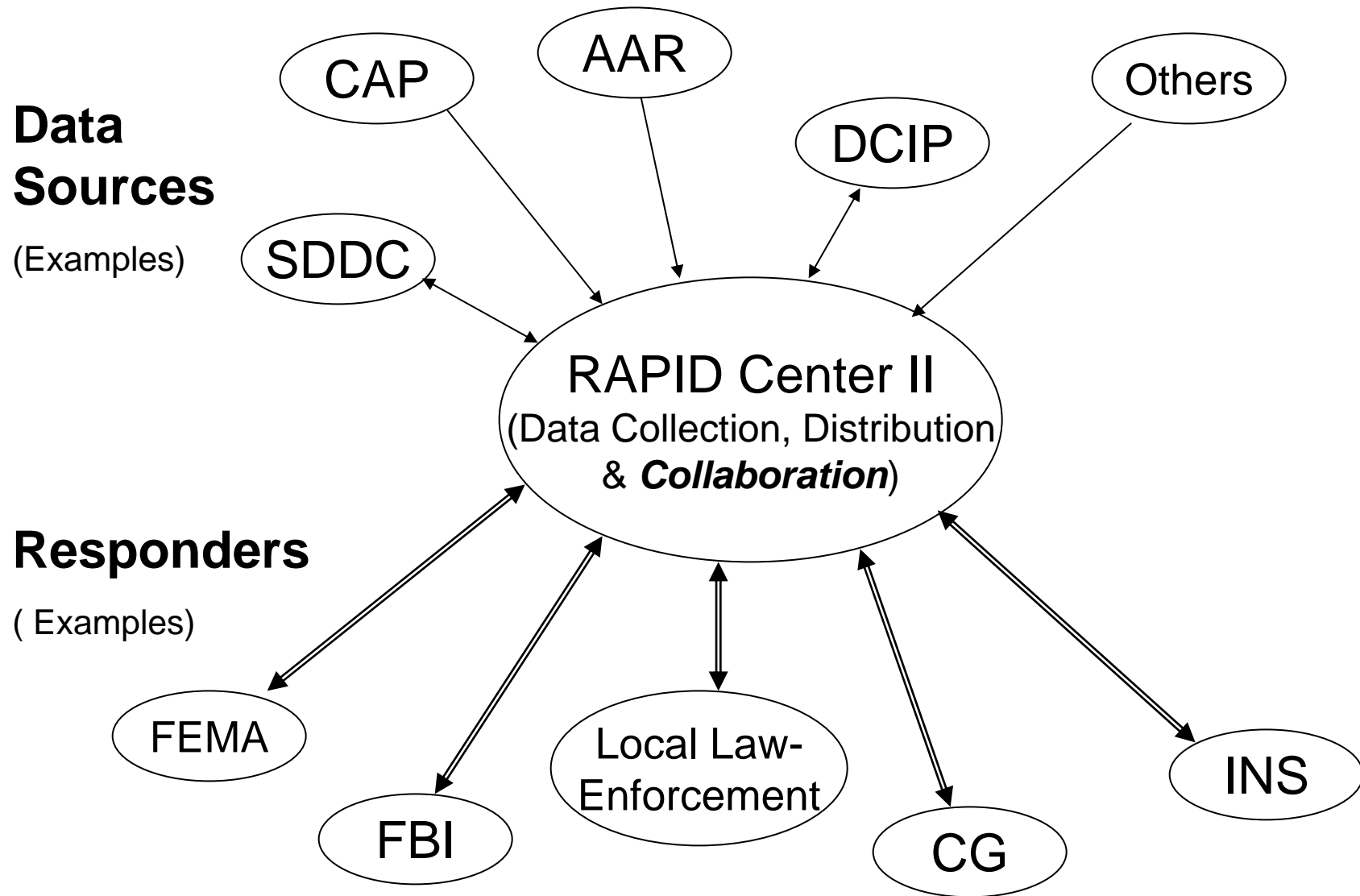
A VIRTUAL COLLABORATION CAPABILITY

RAPID Center is an information hub whose spokes are made up of many people who must respond to a disaster. Because these people can connect to RAPID System, Rapid Center is uniquely situated to support the collaboration necessary to facilitate a rapid and efficient response.

Generally, when responding to a disaster or attempting to prevent one, responders have little time to physically

meet for collaboration. One effective way to plan from a distance is through use of information technology to create a virtual meeting facility, for example, by using PCs and mobile devices connected by way of the Internet to a website with collaboration tools. These tools, which allow users with appropriate permission to see and hear each other as well as to share information in real-time, can provide the necessary collaborative capability. This capability could be added to RAPID System.

A VIRTUAL COLLABORATION CAPABILITY

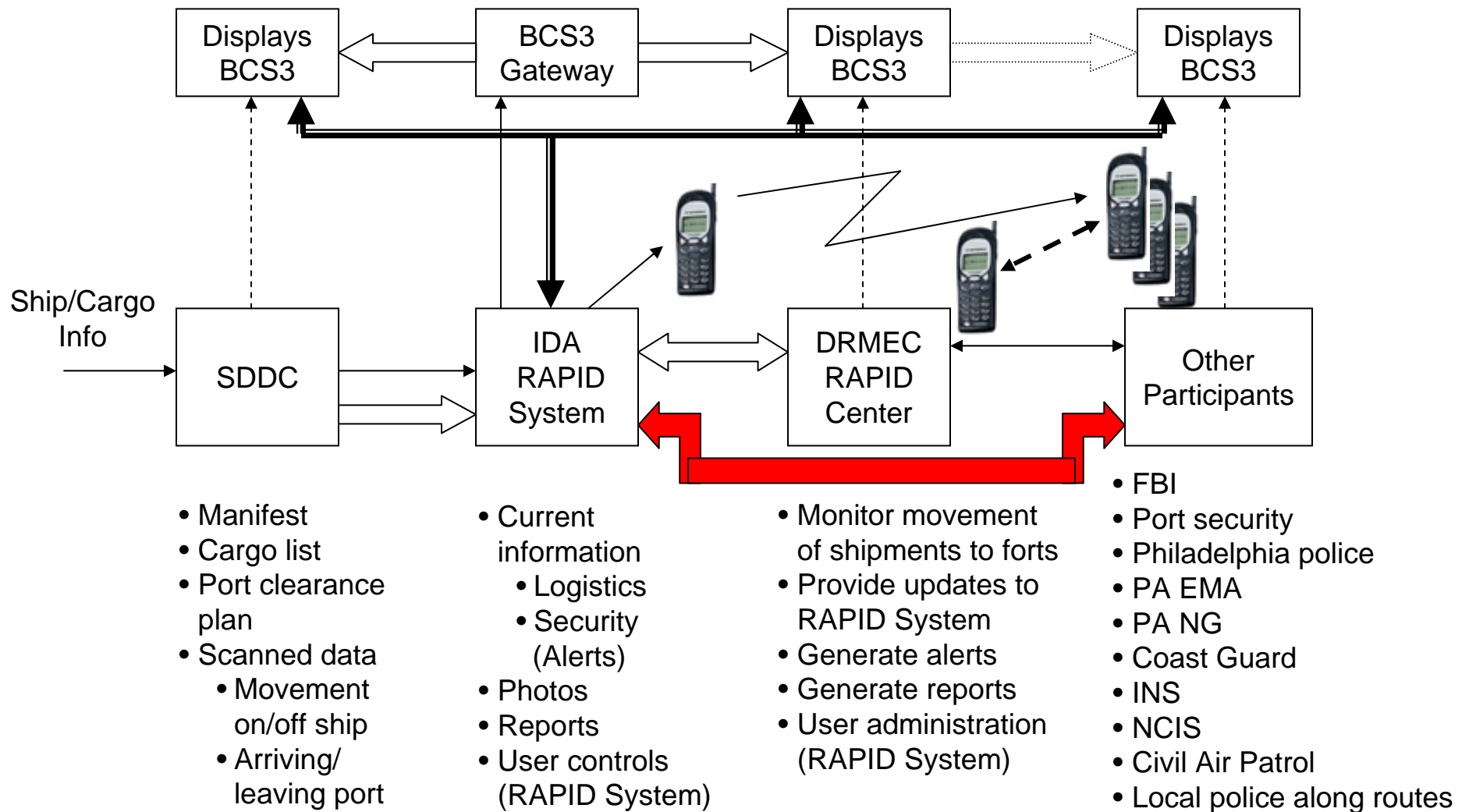


INTEGRATION INTO CURRENT EFFORT

This diagram shows an overview of the information flow in the first two demonstrations. Of specific interest is the connection between “Other Participants” and the RAPID System shown in red. These connections are established as part of the information sharing process. No additional connections need be made when a disaster strikes.

Further, in RAPID System, collaboration sessions would be quick and easy to setup or join. It would take only a click or two and the collaboration facility, which is already an integral part of RAPID System, will display a web page with all of the collaboration capability ready to use. This will be illustrated later.

INTEGRATION INTO CURRENT EFFORT



EXAMPLE OF A COLLABORATION ENVIRONMENT

This screen shot shows an example of a collaboration environment with windows from six modules. All participants see the same windows and the changes that occur on them. A participant's ability to modify what is contained in each window is under the control of the person hosting the meeting. Modules can be added or deleted and their windows resized to meet the needs of the meeting.

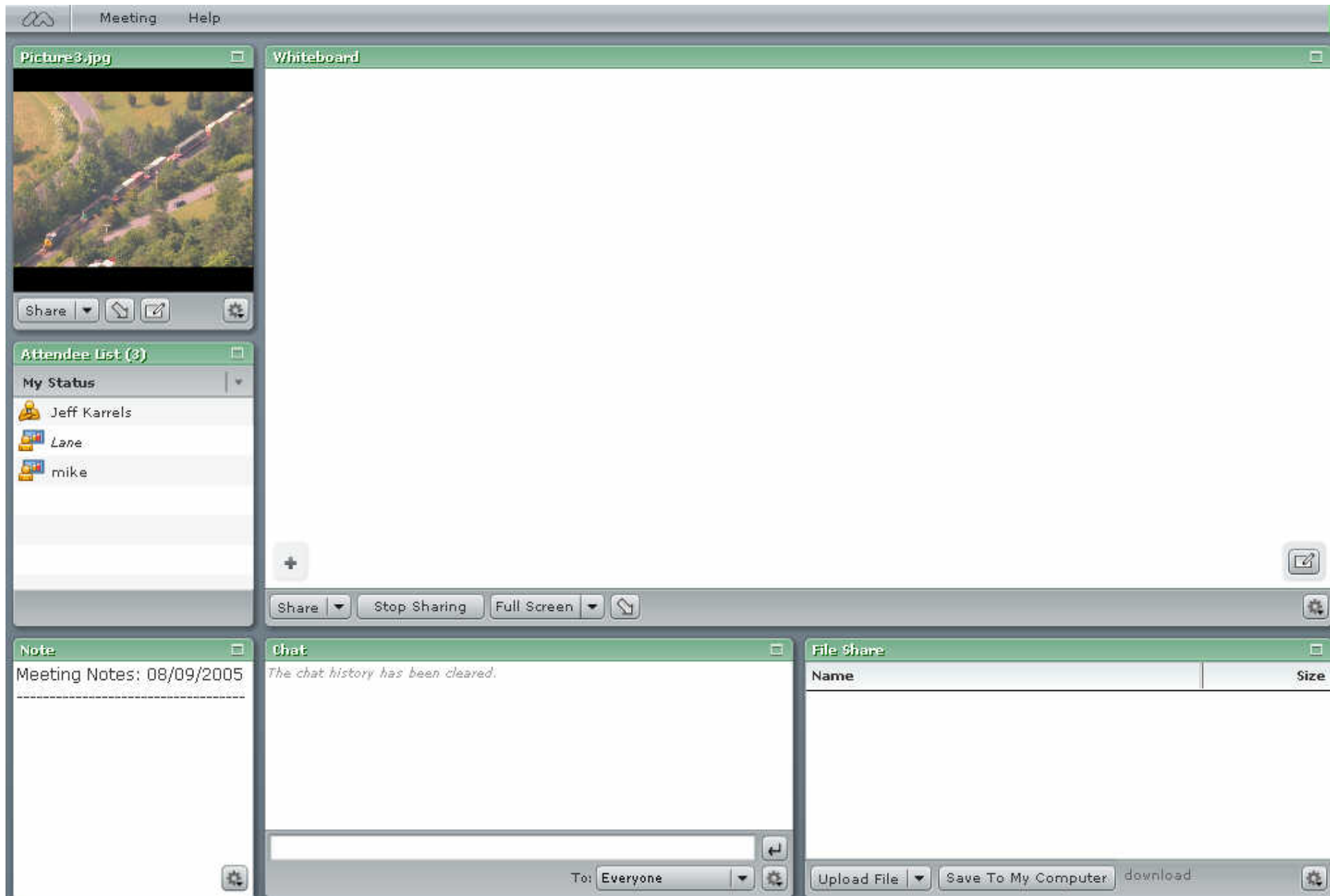
The largest window shown is called a whiteboard. One can draw on the whiteboard or place images on it and draw on them. A toolbar with a number of tools including arrows, line drawing, and marker capability is available to support the discussion.

The upper-left-hand corner contains a picture module. The pictures may be a photos or streaming video.

Below the picture module is participant list. Below that is a module that can contain notes from meetings.

To the right of the notes module is a chat module. The top part of the window shows what the participants have typed in, and this is made available to the person viewing the display. It also shows the name of the participant who entered the text. To enter text one simply clicks on the lower box, types, and, when finished, clicks on the return symbol at the right of the box.

To the right of the chat window is a window for the file sharing module. Here one can place files that participants can download at their convenience.



EXAMPLE OF A COLLABORATION ENVIRONMENT (Continued)

This screen shows examples the different windows might contain. For example, this whiteboard contains a map showing a section of a route the train is passing through (the train is the red rectangle in the upper part of the map) and the imagery window contains a picture of the train carrying war materiel.

65

EXAMPLE OF A COLLABORATION ENVIRONMENT (Continued)

In this screen, the map has been replaced by a picture of a river the train will have to cross.

Meeting Help

Picture3.jpg

Share

Attendee List (2)

My Status

Jeff Karrels
 Lane

Picture2.jpg

Share
Stop Sharing
Full Screen

Note

Meeting Notes: 08/09/2005

Chat

The chat history has been cleared.

To: Everyone

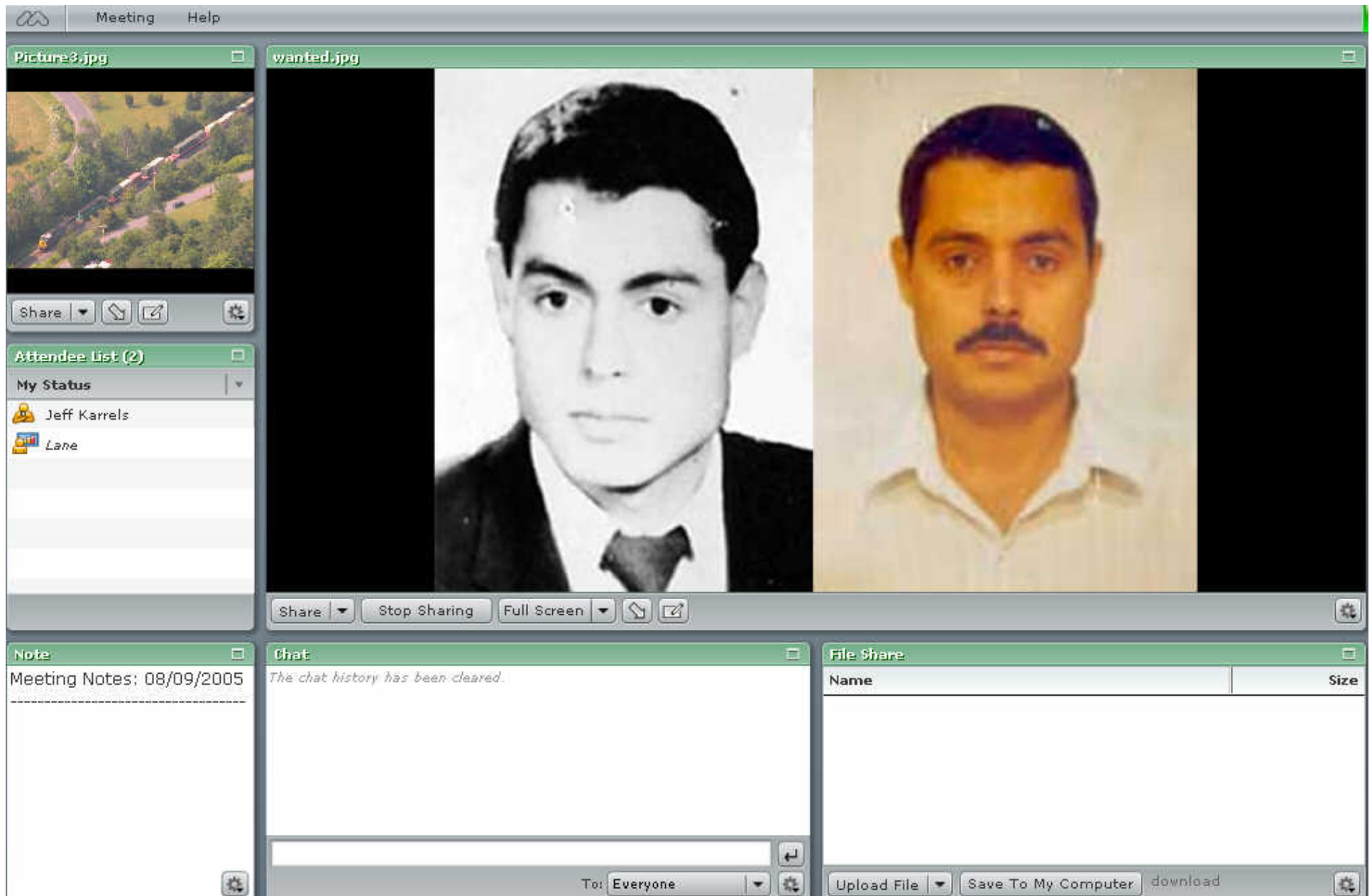
File Share

Name	Size

Upload File
Save To My Computer
download

EXAMPLE OF A COLLABORATION ENVIRONMENT (Continued)

This screen provides actual pictures of a person wanted by the FBI. He could be someone that one of the stakeholders saw around a bridge or some other object of interest. The pictures could be sent out to responders' mobile phones to sensitize all eyes and ears in the field.



Actual photos from FBI wanted list.

SOME STEPS IN ADDING A COLLABORATION ENVIRONMENT

Several initial steps should be taken to develop a collaboration environment. First, such development needs to be shown as feasible by establishing a disaster scenario for test and evaluation. Then, requirements to support collaboration in that scenario should be identified. Next, an environment with at least the basic capability should be integrated into RAPID System with the resulting system evaluated against the requirements. Integration should be such that one can quickly get to the environment. The environment should clearly add to any collaboration capability responders might currently use such as phone calls. Consideration should be given to augmenting individual phone calls with a conference call capability. The next phase would involve sharing graphics type data using the environment.

A second step is to convince others, including stakeholders and responders, that the approach is practical.

This should include not only the environment's capability and ease of use, but its responsiveness and cost as well. The approach preferred here is to provide hands-on demonstrations, in which those for whom the demonstration is being provided are participants.

A third step, which may actually be done in connection with step two, is to ascertain the viability of the approach. That is, the team needs to determine the responders' collaboration requirements when responding to disasters, how the responders see those requirements being met, and how the basic system might be modified to support their needs.

Additional information on potential next steps can be found in Appendix D, RAPID Center II – Improving Disaster Response Through Collaboration.

SOME STEPS IN ADDING A COLLABORATION ENVIRONMENT

Show that it is feasible:

- Establish disaster scenario to test against
- Identify basic requirements for the collaboration environment to support the scenario
- Design, build, integrate, and test a basic environment
- Assess procedure – Initial phone call, to conference line, maintained for audio; Internet collaboration added for graphics

Convince others that it is practical:

- Demo basic system

Ascertain Viability:

- How well does demo meet responders needs?

(This page is intentionally blank.)

Appendix A

THE DRMEC ORGANIZATION

Appendix A

DELAWARE RIVER MARITIME ENTERPRISE COUNCIL (DRMEC)

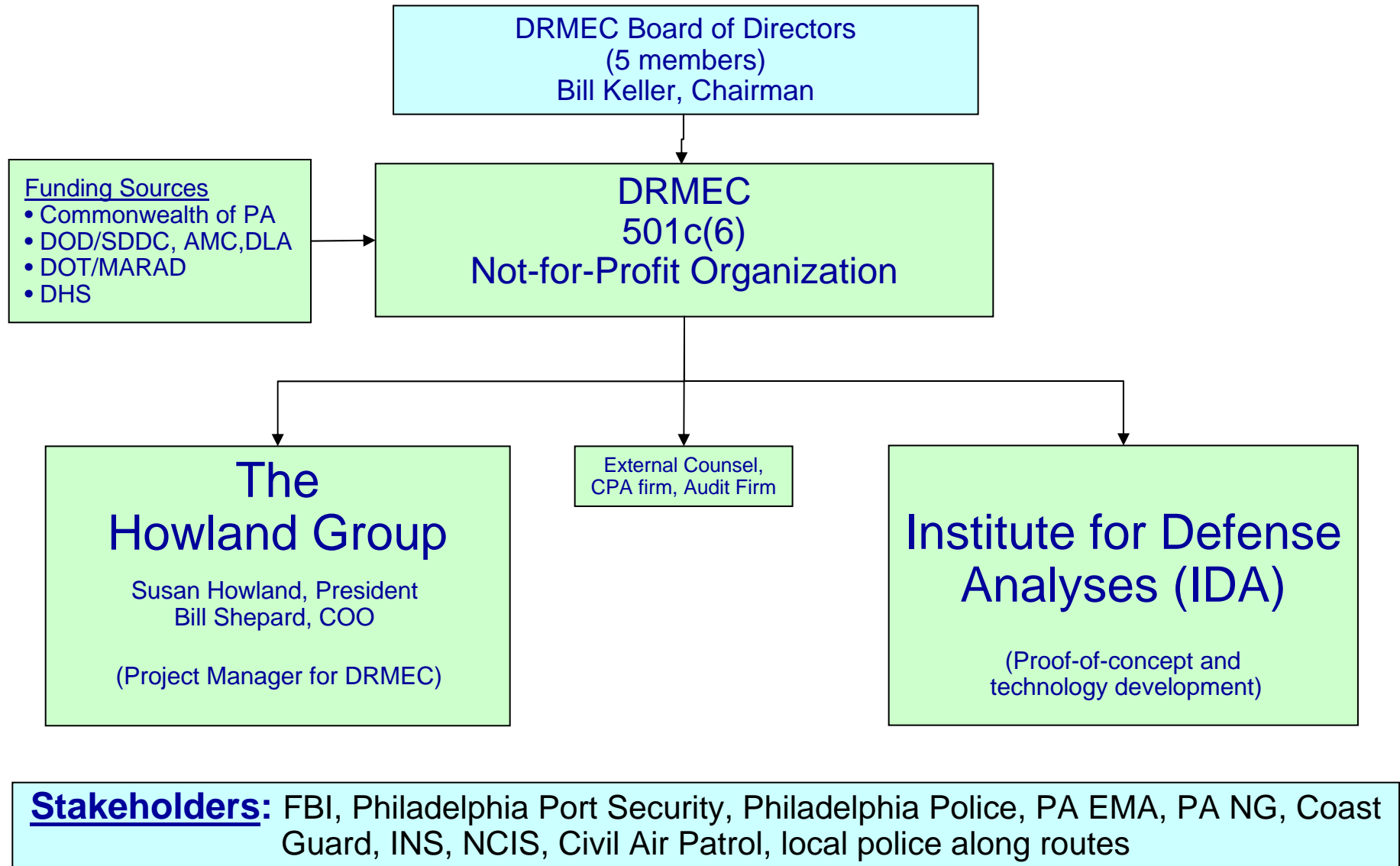
DRMEC is a Pennsylvania not-for-profit organization established to develop rapid and secure end-to-end supply chains for DoD as well as commercial shippers, especially for those shipments passing through sea ports. Its board includes senior members from the Pennsylvania State House of Representatives, the Philadelphia Regional Port Authority, and Reed Smith, an international law firm.

The Howland Group (THG) provides project management services for DRMEC. In addition to developing the concept for RAPID Center, THG interfaces with the many stakeholders which include DoD, DHS, DoT, FBI, Philadelphia Port Security,

Philadelphia Police Department, Pennsylvania Emergency Management Agency (PA EMA), Pennsylvania National Guard (PA NG), U.S. Coast Guard, U.S. Immigration and Naturalization Service (INS), Naval Criminal Investigative Service (NCIS), Civil Air Patrol, railroad personnel, and the local law enforcement organizations, including the local police departments along routes used to move war materiel.

DRMEC has received funding to complete its missions from the Commonwealth of Pennsylvania, DoD [SDDC, Army Materiel Command (AMC) and Defense Logistics Agency (DLA)], DoT (MARAD) and DHS.

Delaware River Maritime Enterprise Council (DRMEC)



(This page intentionally left blank.)

Appendix B

INFORMATION DISTRIBUTION SUPPORT SYSTEM (IDSS)

Appendix B

INFORMATION DISTRIBUTION SUPPORT SYSTEM

This appendix provides basic information on IDA's IDSS system—the platform on which RAPID System is built. The information includes what IDSS is, when and why the effort was started, its design philosophy, and examples of the tasks it performs.

IDSS originally stood for Interoperability Decision Support System. However, as shown here, the letters IDSS have been used as the short name for a number of tasks, all of which have involved the utilization and expansion of the concept of the original IDSS system.

In the timeframe in which the idea for IDSS was conceived, each new computer-based information system was generally developed from scratch. IDSS was one of the first attempts to develop system software in such a way that it could be reused to build systems to support different objectives and it has continued to do so over the 20 years since the effort began.

IDSS

Interoperability Decision Support System

Intelligence Decision Support System

Intelligence Data Support System

Integrated Data Support System

International Decision Support System

Information Distribution Support System

WHAT, WHY, WHEN, WHERE, & HOW

WHAT IS IDSS?

Software for a computer-based information system can be thought of as having system elements and applications. System elements are those features required to administer the system, such as access controls, user permissions, audit trails, and system administrator controls. These types of features are common to most multi-user systems. IDSS differs in that it was designed from the beginning to support new applications and be easy to modify to look like the system of the organization it is serving.

IDSS expands on the basic system features with additions such as libraries, bulletin boards, hierarchical user

groups with their own administrators and alerts for unvalidated login attempts.

In addition, traffic over the communication links can be encrypted using hardware or software encryption techniques, such as Secure Sockets Layer (SSL) or Public Key Infrastructure (PKI).

Further, IDSS conforms to DoD requirements for C2-level systems. IDSS can be freely used by DoD.

WHAT IS IDSS?

The core elements of the software part of a multi-user information system including:

- Basic Elements
 - Access controls and user permissions
 - System administrator controls
 - Hierarchal user groups with their own administrators
 - Designed to host organization's applications
- Enhancements
 - Libraries and bulletin boards
 - Audit trails
 - Unvalidated login attempt alerts
 - Easily modifiable to look like organization's system
 - Secure links between server and client
 - Conforms to DoD's requirement for C2-level systems
- Other
 - Freely usable by DoD

WHEN AND WHY STARTED?

Early in 1985, the Director for Army Information Systems Command, Control Communications, and Computers (ISC4) asked IDA to initiate an effort to develop a multi-user, dial-in system that could be used to share information on the Army's tactical data systems (TDS) among the developer community as a means of promoting TDS interoperability.

In the middle of 1985, the Director for Theater & Tactical Command, Control, Communications, and

Intelligence (C3I) in the Office of the Secretary of Defense (OSD) tasked IDA to evolve the system in such a way as to eliminate the need to develop an entirely new system every time DoD needed to put a new application online. This was accomplished by separating the system functions from the applications, bundling the system functions into a reusable package, and designing that package so that new applications could easily be added.

WHEN AND WHY STARTED?

- Started in early 1985 at the request of Director for Army ISC4
 - As a means of sharing information on Army tactical data system interoperability among the many users
- OSD Director for Theater & Tactical C3I added tasking in mid-1985
 - To eliminate the need to develop an entirely new system every time DoD needs to put a new application online

WHEN AND WHY STARTED? (Continued)

About a year later, the Deputy Under Secretary of Defense (DUSD) for International Programs and Technology tasked IDA to continue to evolve the system to meet the needs of those in the Office of Defense

Cooperation, which fill posts around the world. This tasking emphasized the efficient use of emerging, inexpensive communications technology.

WHEN AND WHY STARTED? (Continued)

- DUSD for International Programs and Technology added tasking in mid-1986
 - To support the Office of Defense Cooperation by developing an inexpensive system:
 - Capable of supporting users worldwide
 - That makes efficient use of emerging, inexpensive communications technology

HOW IS IT DESIGNED?

From the beginning IDSS was intended to be a system inexpensive to both develop and maintain. As a result, a PC with a Microsoft operating system was selected as the platform and a database management system (DBMS) as the programming environment. In the original configuration, the PC was an IBM XT, the operating system was DOS, and the DBMS was Dbase II.

Since then IDSS has run on many different sets of hardware under many different operating systems and has been written in a number of DBMS languages. However, the inexpensive philosophy still holds. Today, IDSS-based systems continue to run on PCs or server versions of PCs, continue to run under various versions of Microsoft Windows, and are currently written in FoxPro and FoxWeb.

When IDSS was first being developed, the 1200-baud modem was just emerging. Using these modems, IDSS was able to support two users at the same time on an XT. As faster modems became available, they were added. As multi-user hardware and software emerged, a single PC-based system was able to support more than 64 simultaneous users. When packet-switching emerged, this capability was also added. SITA, which is used by the airlines and therefore has a presence at every international airport in the world, helped IDSS establish a true around-the-world capability. As IDSS became acceptable to be used on State Department turf, the Department's Black Packet communications system was added. When the Internet emerged, IDSS was modified to operate with it.

HOW IS IT DESIGNED?

- Database oriented
- Currently written in FoxPro and FoxWeb
- Currently runs on Microsoft Windows OS
- Hardware independent
- Communications network independent
 - Telephone lines—Direct and dial-up
 - Packet Switching (Cable & Wireless, SITA)
 - State Department's Black Packet
 - Internet

WHERE HAS IT BEEN USED?

Many organizations in and out of DoD have used IDSS. One of the first was the Military Communications & Electronics Board (MCEB). This was followed by the Office of Defense Cooperation (ODC). This was significant in that many of the users were in U.S. embassies. Thus, IDSS became the first and perhaps the only external computer system to be approved by the State Department for use by users residing in a State Department facility.

Utilization of IDSS in support of the Conventional Forces Reduction in Europe Treaty represented another significant milestone for a number of reasons. First, Russia unexpectedly agreed to sign the treaty creating an immediate need for a comprehensive system to support the complex requirements of the treaty. The developer of the “operational” system needed 2-1/2 years to field it. OSD turned to IDA which, using IDSS, had the first elements of the treaty system in place in 30 days. IDSS was used for the 2-1/2 years it took for the “operational” system to become operational. Second, the treaty required a Secret-level system. IDSS was certified to operate at that level. Third, the crypto selected to support the treaty effort was the STU III. However, the noise on the German telephone

lines made this impossible because the device has no error detection and correction to overcome the noise during data transmission. IDA worked with AT&T to develop crypto with the necessary error detection and correction to ensure the data were correctly transmitted. The first device was called the Secure Data Device (SDD) 1900. IDA continued to work with AT&T to develop an improved version, called the SDD 1910, to more fully meet the needs of the treaty system.

DISA, DLA, and J8 of the Joint Staff (JS) also used IDSS. However, the longest and most extensive use of IDSS has been by Defense Security Cooperation Agency (DSCA). This system, referred to as SAN Web, supports more than 1,000 users in more than 140 countries. It is unique in that it has operated 24/7 for more than 10 years and is still expanding in the applications that it supports. It is the one system that has lived through all of the communications enhancements.

RAPID System takes advantage of all that has been done in the development of IDSS including the ability to make it look like a DRMEC system, the ability to quickly incorporate changes, and the stability of a mature system.

WHERE HAS IT BEEN USED?

Examples

- Military Communications & Electronics Board (MCEB)
- OSD ODC (with State Dept approval)
- Conventional Forces Reduction in Europe Treaty (S)
- DISA (S)
- DLA
- JS/J8 (S)
- SAN Web
- RAPID System

(S) Indicates IDSS system operating at Secret level.

WHAT IDSS ELEMENTS ARE USED IN RAPID SYSTEM?

As shown by the checkmarks, nearly all IDSS core elements are used in RAPID System. The notable exception is Libraries and Bulletin Boards. Due to the transient nature of the demonstrations RAPID Center/RAPID System are being used in, the need for libraries and bulletin boards has not developed.

One can also question the need for RAPID System to conform to DoD's requirement for C2-level systems. However, there is no need to reduce IDSS capability and with DoD's current interest in expanding RAPID Center's responsibilities, there may soon be a need to operate RAPID System at the C2 level.

WHAT IDSS ELEMENTS ARE USED IN RAPID SYSTEM?

- Basic Elements
 - ✓ Access controls and user permissions
 - ✓ System administrator controls
 - ✓ Hierarchal user groups with administrators
- Enhancements
 - Libraries and bulletin boards
 - ✓ Audit trails
 - ✓ Unvalidated login attempt alerts
 - ✓ PKI compatible – server and client
 - Conforms to DoD's requirement for C2 level systems
- Other Features
 - ✓ Freely usable by DoD
 - ✓ Easily modifiable to look like organization's system
 - ✓ Ready to support organization's applications
 - ✓ Used
 - Not Used

HOW IDSS SUPPORTS RAPID SYSTEM

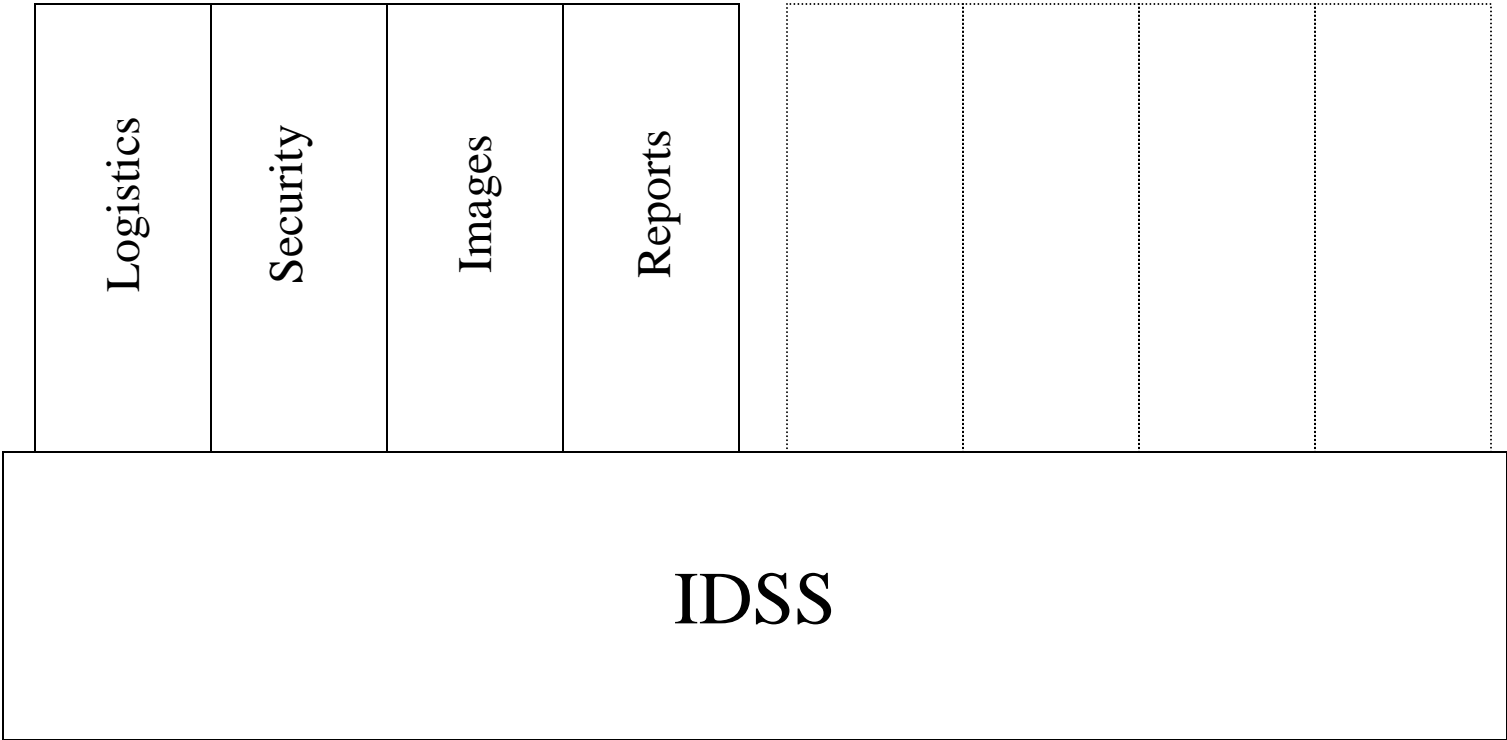
As previously noted, RAPID System is based on IDA's IDSS, which is a standard set of software that provides all basic functions required to operate a wide area multi-user system.

IDSS is designed to host organization's applications. As shown here, modules to support the

needs of logistics, security, imagery, and reports have been added to the IDSS to create RAPID System. Modules run as applications from the main menu. Modules on the right side of the system indicate IDSS' designed-in expansion capability.

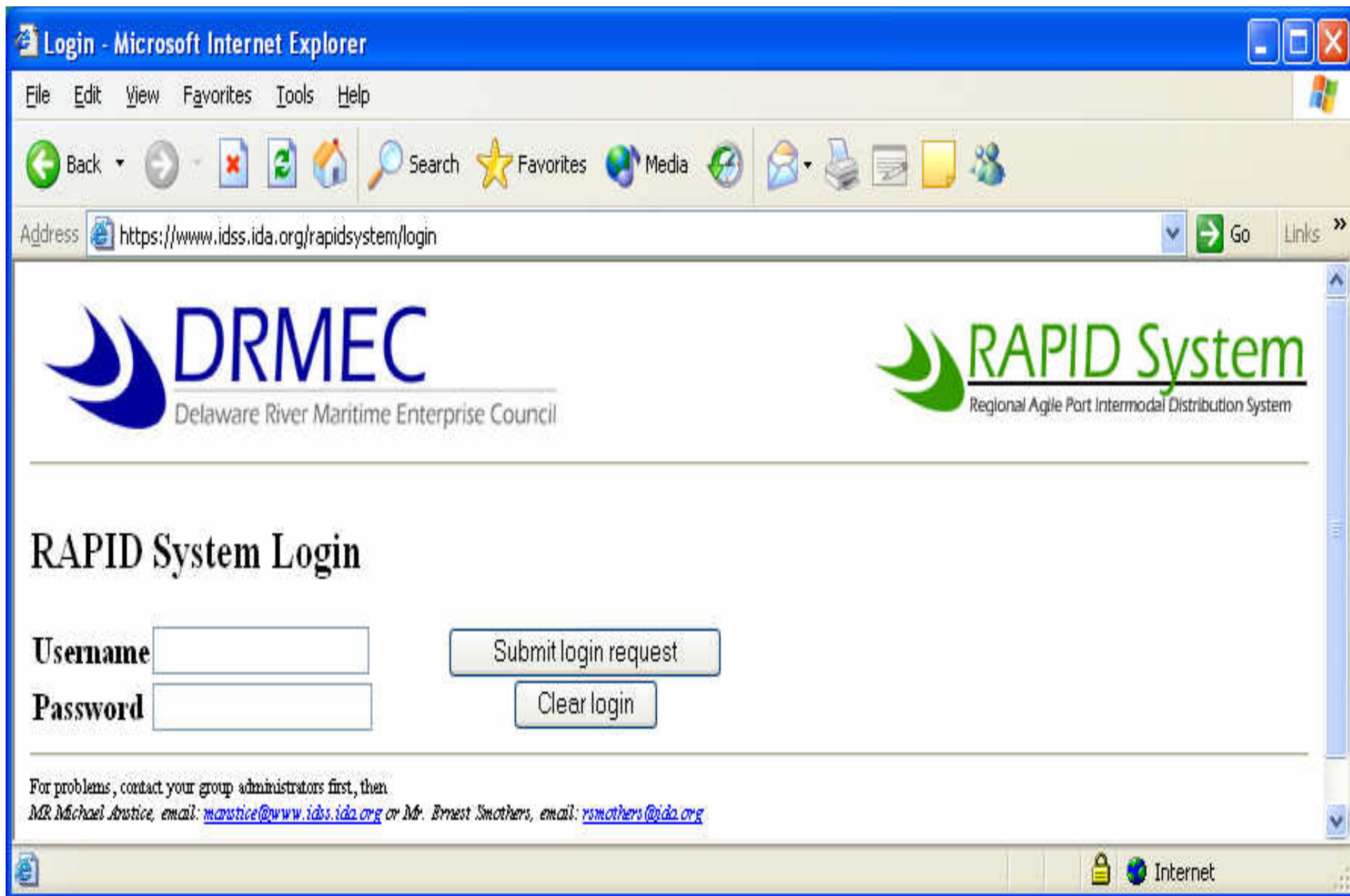
HOW IDSS SUPPORTS RAPID SYSTEM

Application Modules



RAPID SYSTEM LOGIN SCREEN

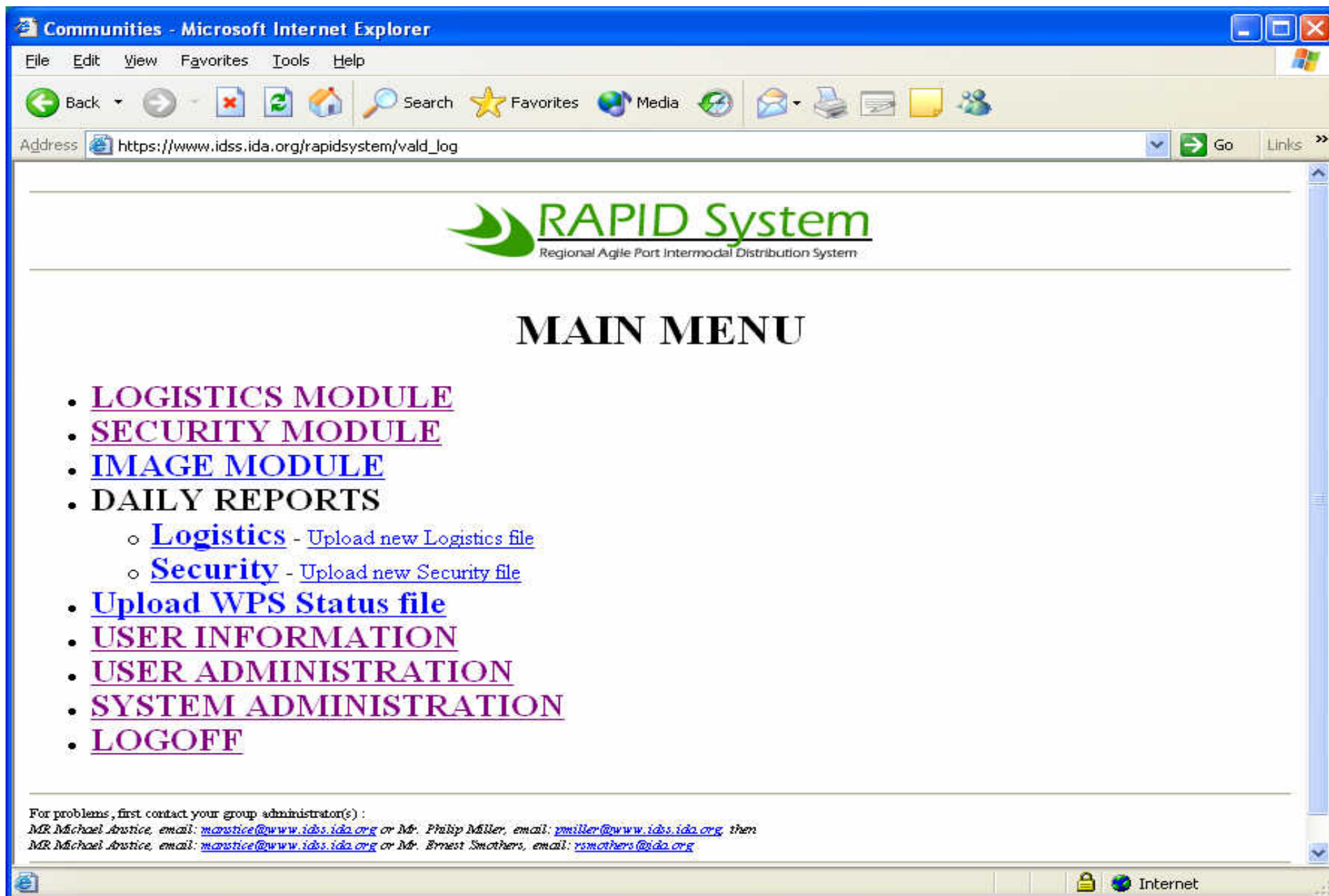
This is the RAPID System login screen. Here the user enters his or her username and password. Note the DRMEC and RAPID System logos show that the website is indeed DRMEC's RAPID System.



RAPID SYSTEM MAIN MENU

As the main menu for RAPID System, this screen provides access to the logistics, security, image, and reports modules as well as the modules for user information and user and system administration. It also provides module

access to permit an authorized user to upload a Worldwide Port System (WPS) status file to update logistics data (the cargo list).



(This page intentionally left blank.)

Appendix C

ADDITIONAL VIEWS FROM THE FIRST DEMONSTRATION

PHOTOS

This appendix contains additional pictures from the first demonstration. The topics are:

- Ship at the dock
- Army truck being offloaded
- Cargo staging area
- RAPID Center 1
- RAPID Center 2

The first three pictures show the area around the port of Philadelphia.

The first picture shows the ship tied up at the dock. Some war materiel is visible on its decks, and containers

stored at the port are shown in the background. Most are commercial containers waiting to be placed on ships or transported to their inland destinations.

The second picture shows an Army truck being driven off the ship. The ID tags with the bar codes are clearly visible just in front of and below the driver.

The third picture is of the Pier 98 Annex, which was used to store the cargo until it could be loaded onto its designated transportation means for shipment to its designated fort.





C-4

Pier 98 Annex Used for Cargo Staging



PHOTOS OF RAPID CENTER

These pictures were taken inside of the three-wide trailer, which housed RAPID Center during the first demonstration of RAPID System.

The first picture shows some of the RAPID Center work areas with the BCS3 displays. The area behind the temporary wall is the SDDC work area.

The second picture shows an ongoing meeting with attention being directed to information on the BCS3 display.





C-8

Appendix D

RAPID CENTER II – IMPROVING DISASTER RESPONSE THROUGH COLLABORATION

Appendix D

RAPID CENTER II

The objective of this appendix is to describe, in some detail, the utility and limitations of adding a Virtual Collaboration Environment (VCE) to the current system.

We will discuss the operational problem, an operational solution, and a technical objective for the solution, followed by a discussion of the current approach.

This leads into the expanded approach and to the impact of the current communications bandwidths and display sizes on the ability to provide a VCE for mobile responders. The appendix closes with a discussion of some additional issues that need to be addressed.

THE OPERATIONAL PROBLEM

Disasters will continue to occur due to various causes including terrorist attacks, natural phenomena such as weather and earthquakes, and major local problems like traffic accidents involving hazardous material and flooding. Generally, each disaster relief organization knows its job and is anxious to fulfill it. However, in part because disasters do not generally conform to municipal boundaries, the organizations often belong to different hierarchies with no readily available common authority to direct and coordinate the overall effort with the quickness that is needed.

Further, the lack of a common operating picture can lead to an uncoordinated approach even in efforts where organizations are accustomed to working together, especially when dealing with an event having details not previously encountered. Lack of a common operating picture will reduce the overall effectiveness of the disaster relief effort.

Quality, low-cost means of providing an easy to use and informative common operating picture for disaster relief are not readily available.

THE OPERATIONAL PROBLEM

- Disasters will occur due to various causes including terrorist attacks, natural phenomena, and major local problems.
- Generally, each disaster relief organization knows its job and is anxious to fulfill it.
- However, they often belong to different hierarchies with no readily available common authority to direct and coordinate the overall effort.
- Lack of a common operating picture can lead to an uncoordinated approach, which will reduce the overall effectiveness of the disaster relief.
- Quality, low-cost means to provide a common operating picture for disaster relief are not readily available.

AN OPERATIONAL SOLUTION

People generally work together better when they know how they fit in. Thus, when uniting disparate groups to accomplish a task, the initial objective is to ‘get everyone on the same page as soon as possible and then to keep them there.’ However, getting organizations together physically in the same location is usually not reasonable as time is generally of the essence.

One alternative is to establish a Virtual Collaboration Facility. Such a facility can be ready at the ‘touch of a button.’ With the computer systems and communications bandwidth available even to mobile users today, the need to be physically together to collaborate is greatly diminished. Further, when the physically together group breaks to go to

work, their ability to understand what has been done and collaborate on what still needs to be done diminishes considerably. Not so with those using virtual means. Situation awareness data can be continuously downloaded and viewed by the organizations as they wish. Further collaboration, if needed, can be quickly initiated since physical travel is not involved and all data can be kept current.

Available graphics, such pictures and maps, can help responders quickly share information. Further, a common operating picture coupled with intelligent software could provide a means of assuring that each need is filled and there is no unnecessary duplication.

AN OPERATIONAL SOLUTION

- Provide a means to quickly “get everyone on the same page and keep them there”
- Establish a Virtual Collaboration Facility to provide a:
 - Virtual facility where responders can quickly come together to discuss the problem and establish what needs to be done, to share data, and to observe progress
 - Common Operating Picture driven by the shared data in a form that can be quickly understood, probably graphic
 - Means to enable each responding organization to define what it expects to do, when and how it expects to do it, and to coordinate its efforts with those of other responders
 - Means to provide assurance that:
 - Each need is filled
 - No unnecessary duplication

TECHNICAL OBJECTIVE

The objective of this effort is to define, develop, and demonstrate a virtual collaboration capability with supporting automation that will facilitate disaster response through data sharing and collaboration. This could easily be done by adding a Virtual Collaboration Facility to the facilities already in RAPID Center. Since RAPID Center is already supported by RAPID System, it would be

reasonable to modify that system to include a virtual collaboration capability. The capability should be specifically designed to and contain those supporting applications which facilitate disaster response through data sharing and collaboration; for example, the ability to share maps and pictures.

TECHNICAL OBJECTIVE

To define, develop, and demonstrate a virtual collaboration facility with supporting automation that will facilitate disaster response through data sharing and collaboration.

COLLABORATION

A number of ways exist to define collaboration. For this effort, the simple definition shown here is preferred.

COLLABORATION

Having independent responders jointly coordinate their efforts to resolve a disaster.

THE CURRENT SITUATION

A. CURRENT APPROACH

A pre-prototype of RAPID Center is currently used in operational situations. The current version is directed toward a specific objective: monitoring the movement of DoD war materiel and alerting stakeholders when significant milestones are reached or when important, unusual, or unexpected events occur. This section briefly describes the current approach and sets the stage for a discussion of an expanded capability.

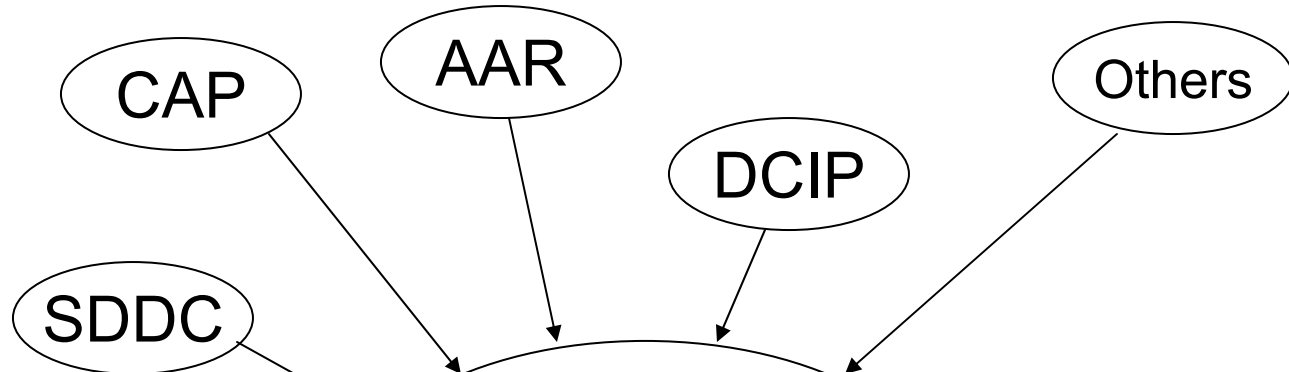
In the current situation, RAPID Center collects data from many sources, arranges it into preplanned formats, and provides that data in meaningful reports for the users

to view. When appropriate, RAPID Center also provides alerts to call user attention to specific events—past or expected. Thus, RAPID Center provides a means to keep users informed. However, in the event the data provided calls attention to a disaster, or to the potential for a disaster, to which some of the users must respond, there is currently no means within RAPID Center for those users to collaborate on actions to be taken beyond a conference call. Since the cargo is generally transported over a number of States, this could lead to missed opportunities to avoid preventable disasters and less than optimum disaster relief for disasters that do occur.

THE CURRENT SITUATION

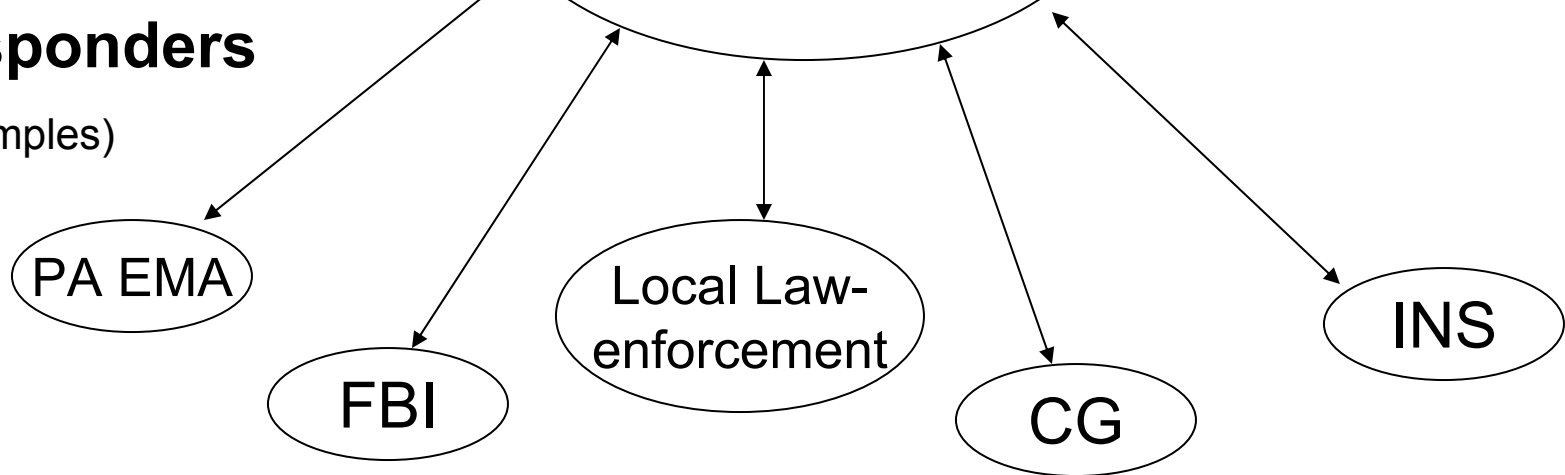
Data Sources

(Examples)



Responders

(Examples)

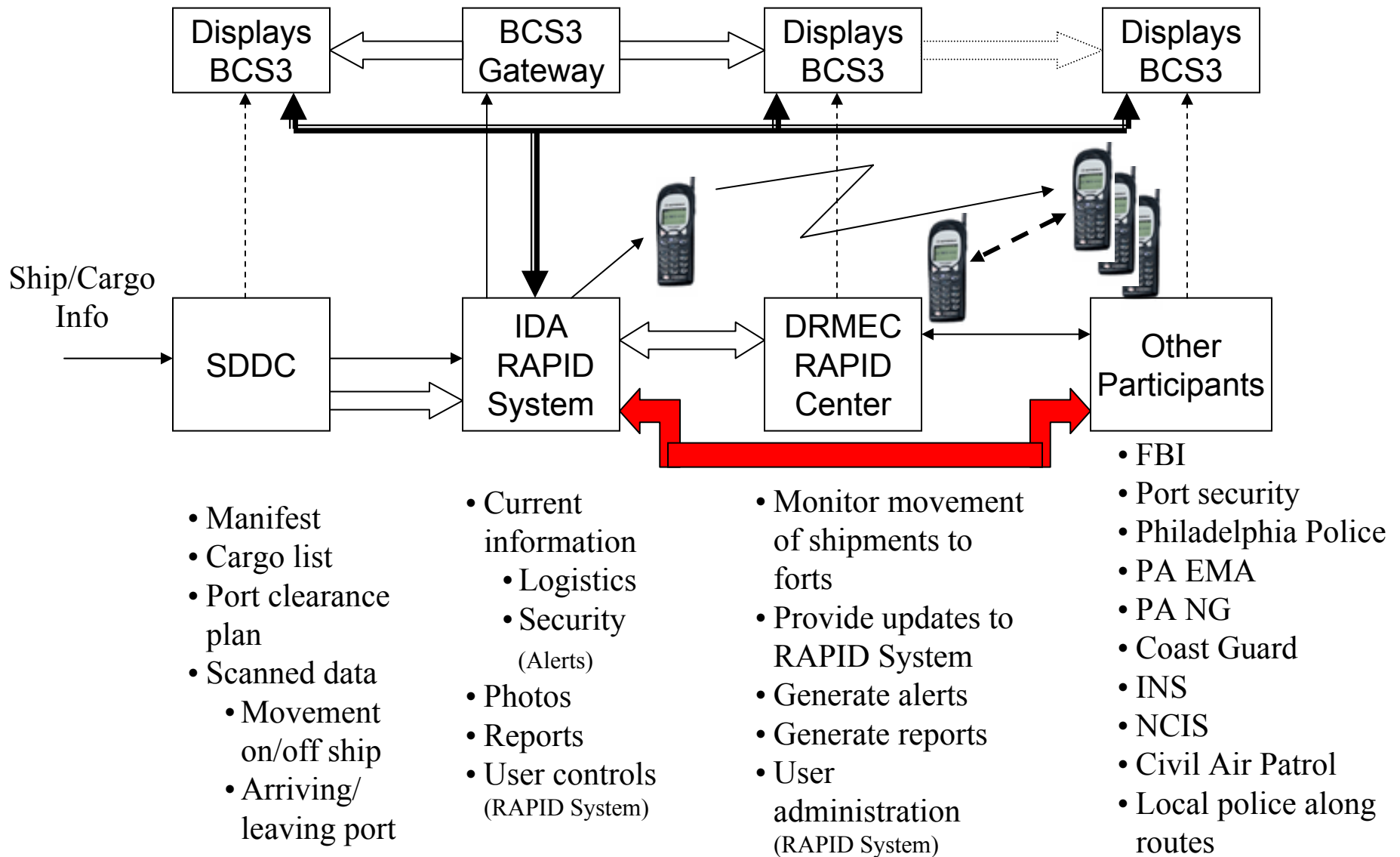


OVERVIEW OF CURRENT EFFORT

This chart shows an overview of the information flow in the (current) effort described previously and in the main body of the report. Of specific interest here is the connection between “Other Participants” and RAPID System (shown in red). These connections are established as part of the information-sharing process. No additional connections need be established when a disaster strikes.

Furthermore, in RAPID System, collaboration sessions are quick and easy to setup or join. It takes only only a click or two and the collaboration facility, which is an integral part of RAPID System, will display a web page with all of the collaboration capability ready to use. This will be illustrated later.

OVERVIEW OF CURRENT EFFORT



A FIRST STEP – ADD A COLLABORATION CAPABILITY

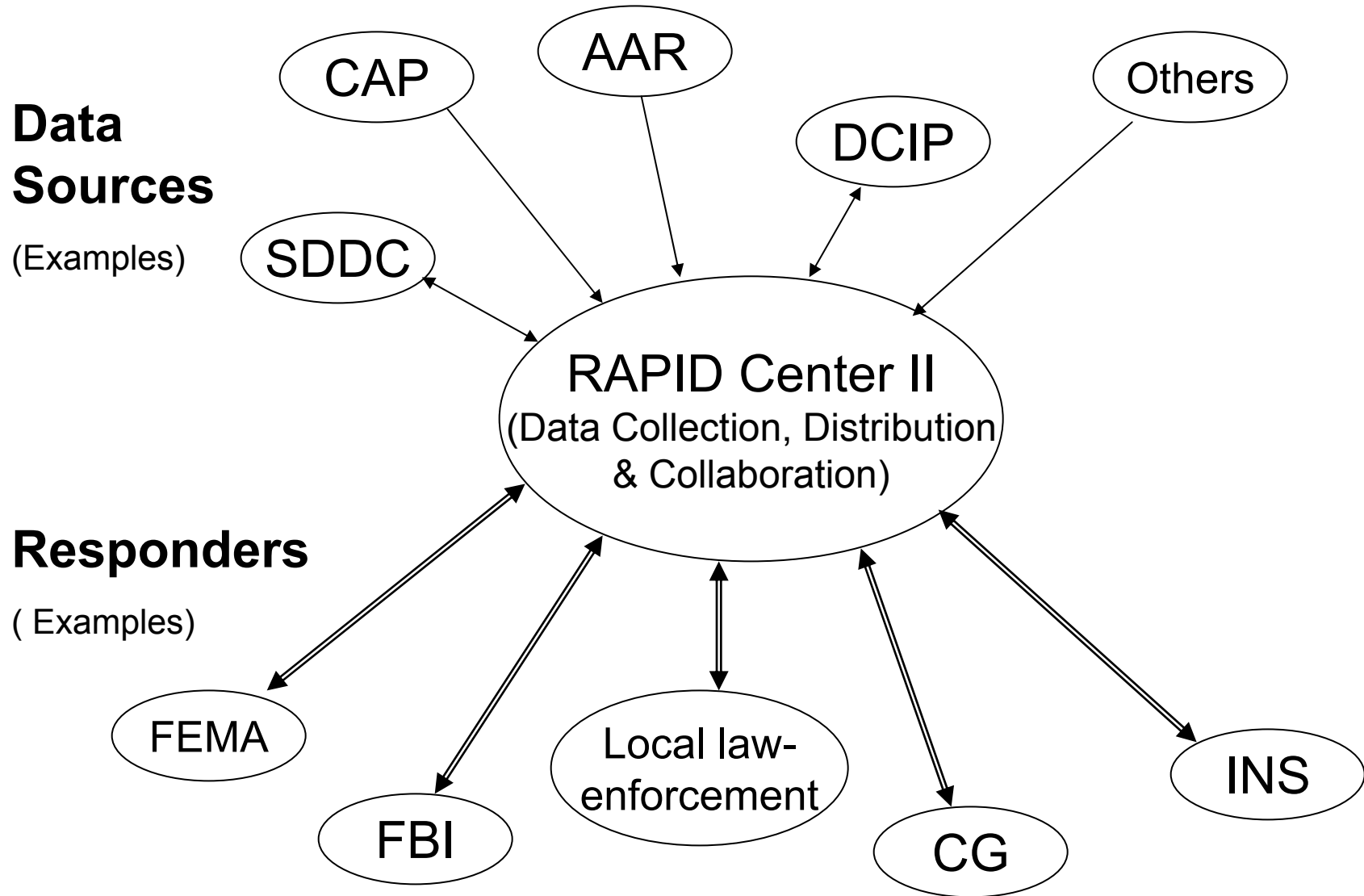
B. EXPANDED APPROACH

RAPID Center is, in fact, an information hub, whose spokes are made up of people who must respond to a disaster. Because these people can connect to RAPID System, RAPID Center is uniquely situated to support the collaboration necessary for the responders to coordinate their efforts to bring about a rapid and efficient response to the disaster.

Generally when responding to a disaster or attempting to prevent one, responders have little time to physically meet

to collaborate. One effective way to plan from a distance is through use of virtual means, for example, by using PCs and mobile devices connected by way of the Internet to a website with collaboration tools. These tools, which allow users with appropriate permission to see and hear each other as well as to share information in real-time, can provide the necessary capability for collaboration. Such a capability could be added to RAPID System.

A FIRST STEP



A MORE GENERAL SITUATION

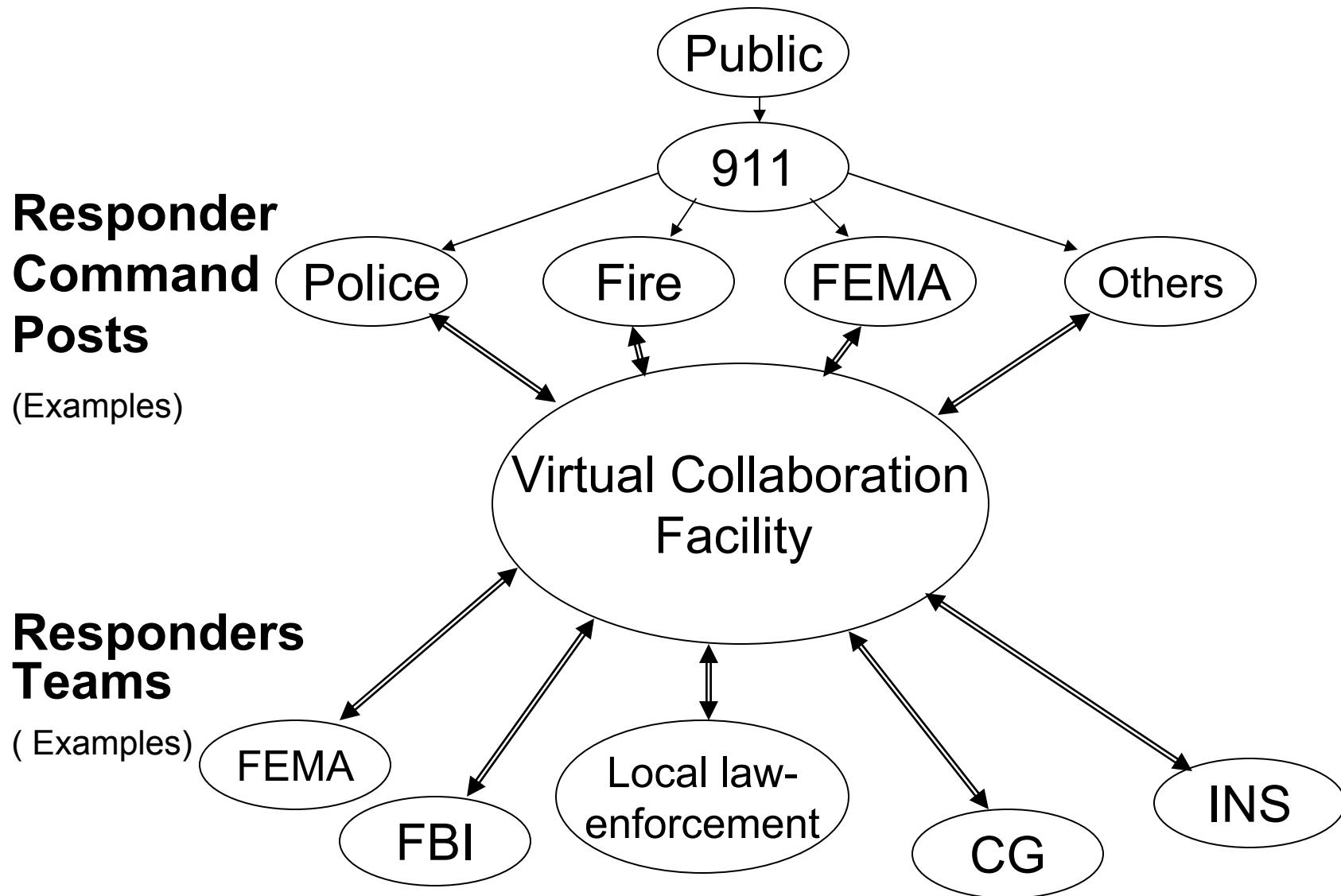
The utility of the collaboration facility is not limited to coordinating the safe movement of DoD cargo. It, as well as a modified version of RAPID System, could be used to support a variety of situations including terrorist attacks, natural disasters, and major local problems such as a hazardous material spill that suddenly causes destruction in an area and requires responders from a number of local jurisdictions.

One can realistically assume that the first indication of such an event might be a 911 call from a citizen who happened to observe the event. In many, if not most locales, this acts as a trigger to connect responders at the command

level—at least by voice. The virtual collaboration facility could add the world of graphics to the support of these situations. Communications and mobile devices have evolved to the point where, at least to some degree, the responder teams are able to be connected to the virtual collaboration facility as well, for example, responders may have laptops equipped with mobile communications capability. Many of those with only mobile phones can also connect to the collaboration facility while all can be sent products from it such as maps, pictures, and text documents. Furthermore, this capability to support the responders will most certainly continue to improve.

A MORE GENERAL SITUATION

For Example: Terrorist Attack, Natural Disaster, Major Local Problem



COMMAND & CONTROL VS. COLLABORATION & COORDINATION

This chart illustrates a notional organization responding to a disaster. FEMA, FBI, Coast Guard, and local law enforcement have been used as examples with a Joint Command Center coordinating their efforts. Each organization is shown with a chief at the command command center, a field commander who is at the scene, and a number of responder teams under his command.

Command and control flows up and down lines within each organization. Examples are mission and timeframe flowing down and reports and requests for additional assets flowing up.

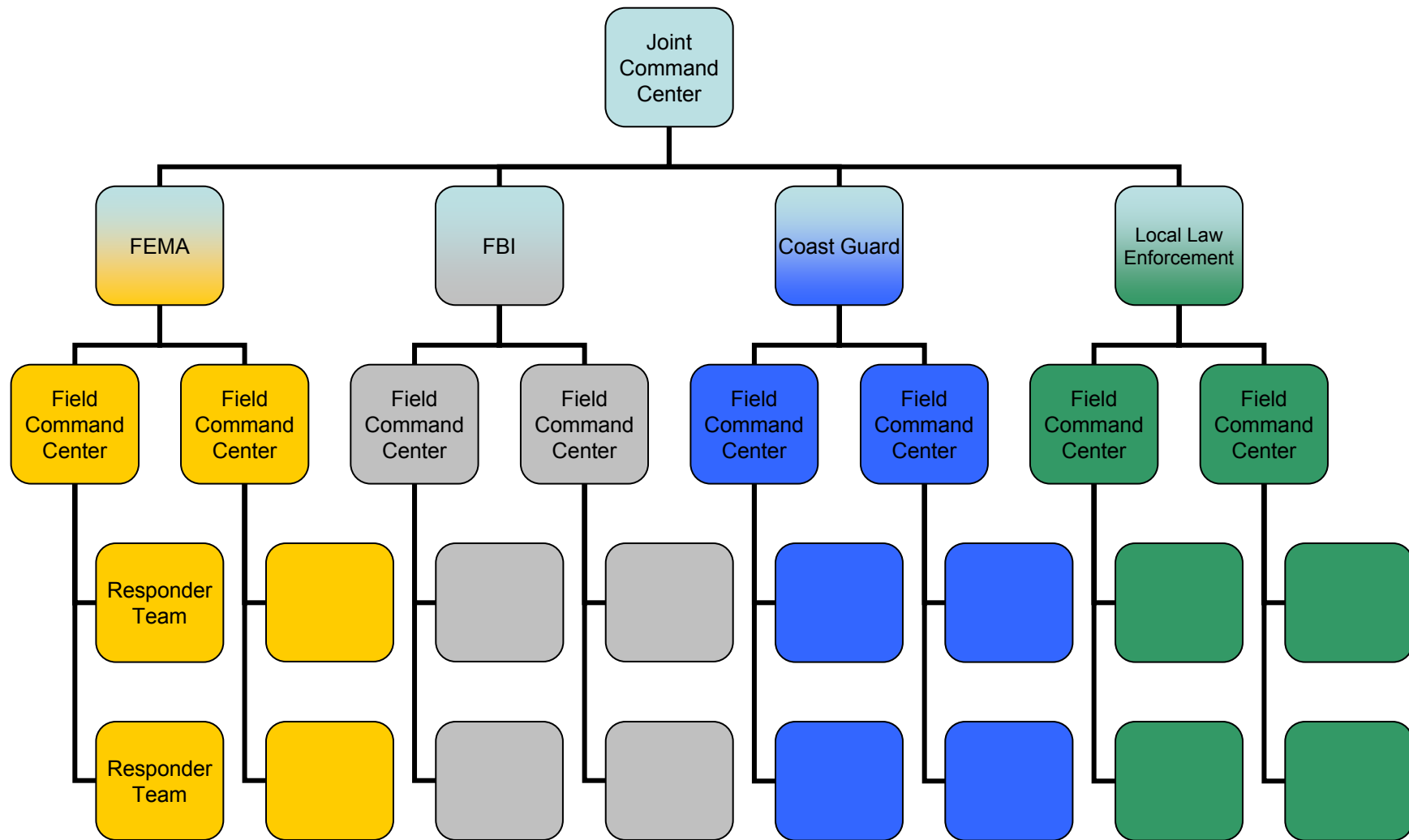
Coordination occurs laterally among entities at the same level where level is not so much determined by normal rank in one's organization, but by its geographic or functional areas of responsibility.

Collaboration needs to occur both within each organization as well as across the organizations. However, in

general, assets to carry out the necessary collaboration are much more likely to be planned for and available within an organization than are the means to carry out collaboration across organizations. When a group of organizations that report through different management chains work together on an effort they tend to work as equals, i.e., one cooperates with, but does not take orders from an equal. An organization controls its resources and continues to do so unless some other arrangement is made. This is shown by the columns, and collaboration does not change that.

On the other hand, assuming responders want to do their job, they need to know how they fit in. Therefore, collaboration and coordination generally go across the organizations (i.e., at the row level). Each level, or row, has its own means and limitations as to how it carries out the collaboration and coordination efforts.

COMMAND & CONTROL VS. COLLABORATION & COORDINATION



SOME COLLABORATIVE MEANS

Some of the means that organizations might use to collaborate are divided into direct contact, shared, and interactive.

Direct contact can be by voice or video. Radios and telephones, including mobile phones, are used to communicate by voice. Many phones are able to conference in additional callers. Conference call services can connect large numbers of callers into one conference. PCs as well as many mobile phones are able to display streaming video.

Documents and imagery can be shared in hard copy as well as electronically.

Interactive here means the users participate. For example, all users may see the same document and one may be able to modify it. Who has the capability to modify the document is generally under the control of the person hosting the meeting. One may also have an electronic sketchpad that users, generally one at a time, can draw on with a variety of electronic tools provided with the software. Some systems permit one to place items such as a map, document, or picture on the sketchpad and allow users to mark on the item with the tools.

SOME COLLABORATIVE MEANS

- Direct Contact
 - Voice
 - Person to Person
 - Conference
 - Video
 - Person to Person
 - Conference
- Shared
 - Documents
 - Imagery
 - Pictures
 - Maps
 - Streaming Video
- Interactive
 - Documents
 - Imagery
 - Graphics
 - Sketchpads with backgrounds (maps & pictures)

IMPACT OF BANDWIDTH & DISPLAY SIZE ON COLLABORATION OPTIONS

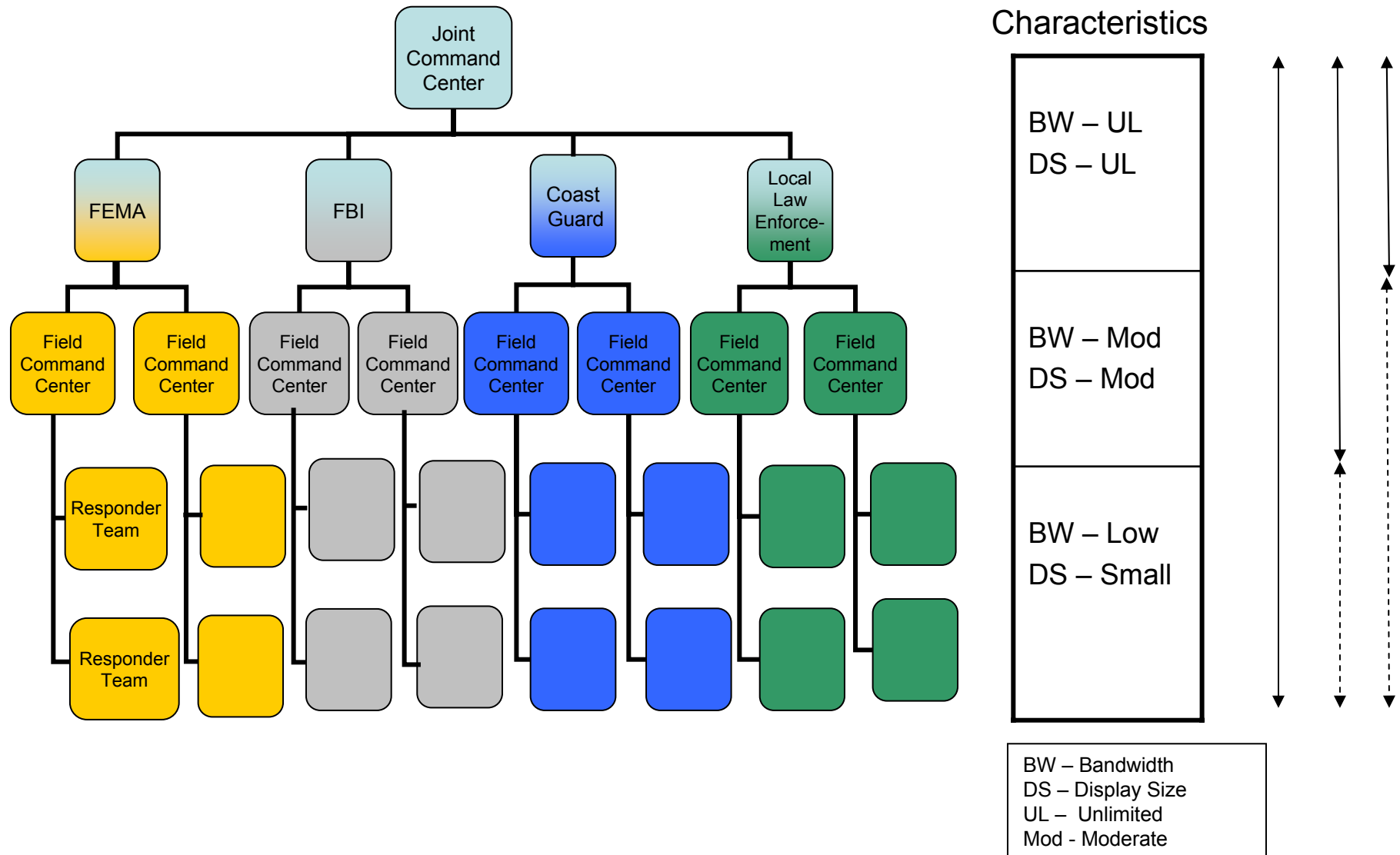
In choosing a means to collaborate, one must be mindful of the limitations imposed by the equipment and the services available (or practical) at the different echelons. Two are shown: bandwidth and display size.

At the command center, level bandwidth and display size are essentially unlimited given that these centers are significant, fixed installations. At the field command post level display size is limited by the size of the vehicle and

bandwidth may be limited by location, available service to mobile units and equipment—especially antenna size.

Response teams may only have handheld radios and mobile phones. Although direct collaboration is available with some, sharing the size of these devices will limit the utility of sending graphics data, and the capabilities of the wireless communications connecting them will limit the bandwidth, which affects the speed with which information can be sent.

IMPACT OF BANDWIDTH & DISPLAY SIZE ON COLLABORATION OPTIONS



COLLABORATIVE MEANS ON THE DESKTOP

Some features could be made available in a desktop virtual collaboration facility. The numbers 1, 2, and 3 could be pictures of users from the organizations one is collaboration with, with additional team members behind the primary. The facility would also have some controls to adjust the display, the functions available, and the user's permissions. The lower part of the chart shows some other features that could be made available. Interactive office tools might include a word

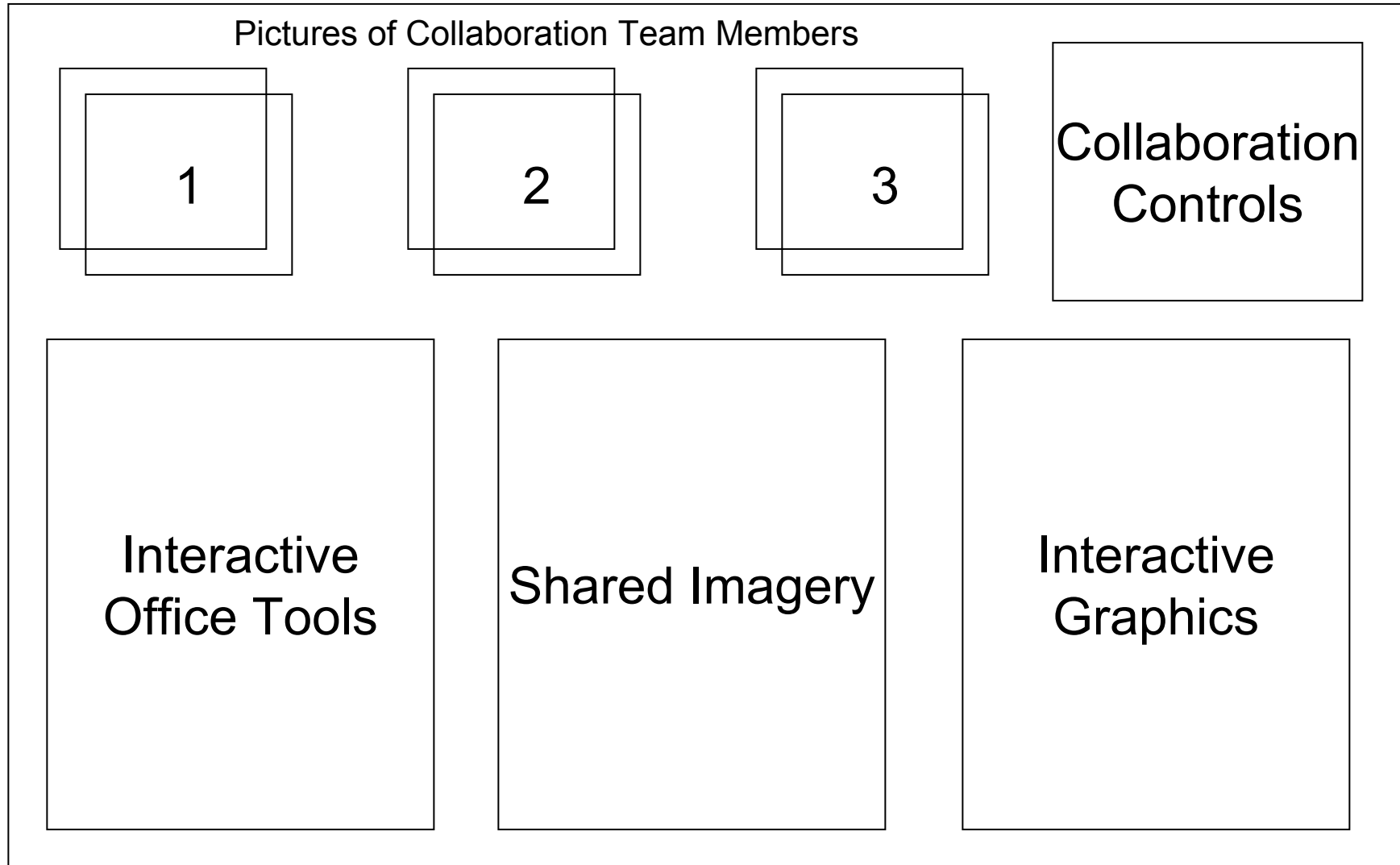
word processor, a spreadsheet, and a database management program.

Shared imagery could include pictures (even those taken using mobile phones in the field) and streaming video.

Interactive graphics would likely include the whiteboard and its capabilities previously discussed.

COLLABORATIVE MEANS ON THE DESKTOP

e.g., COMPASS, Net Meeting....

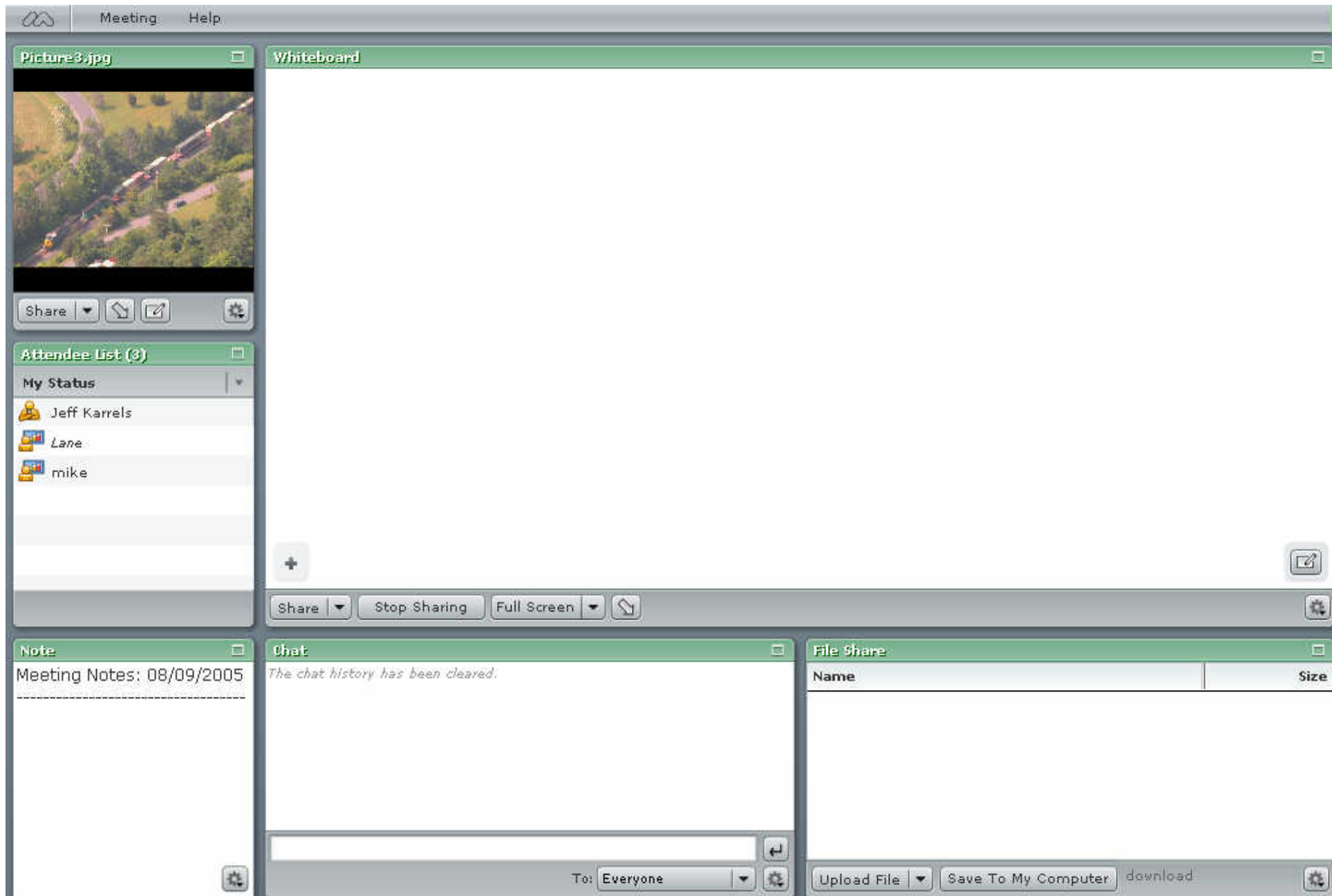


EXAMPLE OF A VIRTUAL COLLABORATION ENVIRONMENT MAIN SCREEN

This is a screen shot of a commercial off-the-shelf (COTS) collaboration environment that has been integrated into RAPID System for demonstration purposes. This version of a collaborative environment is called Breeze, a product of Macromedia corporation. Within its six windows are a large whiteboard with a tool set in the upper right hand corner. The window in the upper left is an imagery window that can display single photos as well as streaming video. The next window down shows the users currently participating in the session. The bottom left window is for meeting notes. The middle window on the

bottom is a chat window. At the bottom right is a window where files can be placed for participants to download. These are only examples of the available features. Additional functions can also be developed and integrated into the environment by the host website team.

The object of this effort is to show stakeholders and potential stakeholders an example of what a virtual collaboration environment might look like, to allow them to work with it, and to obtain their comments on how to modify it to better support their needs.



SOME COLLABORATIVE MEANS FOR MOBILE ENTITIES

Many potential devices could be used by mobile units to participate in the collaboration sessions and provide information coming out of those sessions.

The first three are rather obvious, and the capabilities of the mobile phones and PDAs have already been discussed. However, it is worth noting again that streaming

video is currently being incorporated into mobile phones and PDAs.

Many law enforcement cars are now equipped with laptops. Wearable computers are becoming increasingly available and eye piece displays already provide a virtual display that appears to the eye to be very large in size.

SOME COLLABORATIVE MEANS FOR MOBILE ENTITIES

Types of devices include:

- Radios
- Mobile phones
- PDAs
- Laptops
- Wearable computers with eye piece displays

COLLABORATIVE MEANS FOR MOBILE ENTITIES

As noted before, the bandwidth and display sizes available at the command center level are virtually unlimited. This is not true for the mobile responders. The means available to the mobile user are summarized in terms of three categories: available, available/near-term, and requires research and development (R&D).

The limitations on streaming video (under Shared Imagery) is basically a display-size issue. Streaming video is being incorporated into small devices such as

tiny mobile phones. However, it remains to be seen if this has any value in disaster prevention and relief efforts when the display screen is so small.

The small size of the current mobile phones displays and their controls is also a problem with sketch pads (under Interactive/Graphics). In addition, wireless bandwidth may also need to be improved to make the technique useful in the field.

COLLABORATIVE MEANS FOR MOBILE ENTITIES

Using Mobile Devices

- Direct Contact
 - Voice
 - ✓ Person to Person
 - ✓ Conference
 - Video
 - ♦ Person to Person
 - ♦ Conference
 - Shared
 - ✓ Documents
 - Imagery
 - ✓ Pictures
 - ✓ Maps
 - ♦ Streaming Video
 - Interactive
 - ♦ Documents
 - ♦ Imagery
 - Graphics
 - Sketchpads with backgrounds (maps & pictures)
- ✓ Available
 - ♦ Available/Near-term
 - Requires R & D

POTENTIAL WAYS FORWARD—TECHNICAL PHASES

This chart shows potential ways forward in technical terms or phases. Currently one can expect to deploy systems that have two-dimensional displays and provide documents, maps, photos, video, and messages to users.

With some development, one could add three-dimensional displays. Although three-dimensional devices have been around for some time, development is necessary to adapt them to this environment; software is also needed.

Virtual reality is a powerful technique. Its ability to transport the mind into a virtual situation is spectacular.

Although a significant amount of development in both hardware and software is required, the utility will be worthwhile. The first applications will probably be with helmet displays. Use of holographic techniques may make people who are reluctant to use a helmet more comfortable. Participants will be able to picture who is sitting at one's desk, which now looks like a conference table, with the remaining participants seated around it. Then one can add the capability to show presentations and draw on easels or whiteboards, all in virtual space.

POTENTIAL WAYS FORWARD—TECHNICAL PHASES

Phase	Vision	Devices	Setting Examples
1	2-Dimensional	Current displays	Documents, Maps, Photos, etc.
2	3-Dimensional	Glasses or helmets	Same as 1, but in 3D with rotation & talking heads
3	Virtual Reality	Glasses, helmets, or (physical) open space	Holographic images in conference room

SOME INITIAL STEPS

Several initial steps should be taken in the development of a collaboration environment. First, one must show that the effort is feasible by establishing a disaster scenario for test and evaluation. Then, as a minimum, the obvious requirements to support collaboration in that scenario should be identified. Next, an environment with at least the basic capability should be integrated into RAPID System with the results evaluated against the requirements. Integration should be such that one can quickly get to the environment. The environment should clearly add to any collaboration capability responders might currently use, e.g., phone calls. Consideration should be given to augmenting individual phone calls with a conference call capability. The next phase would involve sharing graphics type data using the virtual collaboration environment.

A second step is to convince others, including stakeholders and responders, that the approach is practical. This should include not only the environment's capability and ease of use, but its responsiveness and cost as well. The approach preferred here is to provide demonstrations, in particular hands-on demonstrations, in which those for whom the demonstration is being provided are participants.

A third step, which may actually be done in connection with step two, is to ascertain the viability of the approach. That is, the team needs to determine the responders' collaboration requirements when responding to disasters, how the responders see those requirements being met and how the basic system might be modified to support their needs.

SOME INITIAL STEPS

- Establish Virtual Collaboration Facility required characteristics
 - Determine:
 - Responder's needs—Survey expected responders
 - Existing capability—Examine existing and planned collaboration facilities & systems
 - Establish detailed concepts for increasing levels of collaboration
 - Determine the level of collaboration beneficial for different levels of disasters
 - Establish operational concept and procedures
 - Determine automation and communication needs
- Define demonstration for pilot version of virtual facility including data sources, responders, center configuration, support system with hardware and software for desktop and mobile devices, and communication needs
- Build, conduct and report-on demonstration
- Initiate research on technology and procedures not available for pilot version

EXAMPLE OF COLLABORATIVE SCENARIO

C. A STARTING POINT

As a first step, let's describe a scenario in which collaboration would be helpful. For example, in a situation where decisions by one organization depend on those of another, which depend on those of the original organization.

This might occur in the following situation. Materiel is to be moved by train from a fort to a port. SDDC determines the cargo to be moved. The rail company determines the train's route, departure time, speed, etc. Disaster Preparedness Office (DPO) has information on infrastructure (gas lines, electrical power generation facilities, etc.), which could be at increased risk if certain

types of materiel passed certain points or if certain events occurred near those points.

To ensure that the selected cargo does not generate any unacceptable risks by being transported over the selected route, DPO is requested to make a risk assessment. To ensure the data needed for the assessment are both available and unchangeable, copies are placed in a 'lockbox' in a collaboration module.

DPO uses the cargo list, the route, and timeframe along with the infrastructure data it holds to assess the risks associated with moving the identified cargo over the specified route during the timeframe provided.

EXAMPLE OF COLLABORATIVE SCENARIO

- Moving materiel from fort to port by train
- SDDC determines cargo to be moved
- Rail company determines train's route and timeframe
- Cargo, route, timeframe, and threat level entered into lockbox in RAPID System's collaboration module
- DPO requested to assess risk of moving cargo over route
- DPO uses infrastructure data to assess risks and enters resulting assessment into lockbox and notifies stakeholders of its availability

EXAMPLE OF COLLABORATIVE SCENARIO (Continued)

The risk assessment would most likely contain different values for different sections of the route. In addition, it should identify the cargo that causes any of the risk values to reach unusually high levels.

As the stakeholders and responders review the risk assessment, there may be a need for clarification. If graphics are needed, the collaboration environment could be used. It is possible that DPO could be asked to redo the assessment with new data. However, in the end, the cargo must be moved to the port. Thus some of the

possible outcomes of the deliberations are: live with the risks, change the train route (although there is only a small chance of this given the limited rail structure), transport the problem cargo by another means (by truck for example), and increase the law enforcement presence in the high-risk areas during the time the train is passing through, and, possibly, for some period of time before the train arrives.

EXAMPLE OF COLLABORATIVE SCENARIO (Continued)

- Risk assessment might include risks for different sections of the route along with the cargo items that cause any increased risk
- Any stakeholder/responder could react to the risk assessment by requesting a 'virtual' meeting with any other stakeholders/responders
- Some possible outcomes include:
 - Live with the risks
 - Change train route
 - Transport problem cargo by other means
 - Increase law enforcement in high-risk areas

SOME COLLABORATIVE ENVIRONMENT CONSIDERATIONS

Addresses here is a special-case collaboration. Where some collaboration might be able to progress at a leisurely pace, let us assume that is not the case here. In these scenarios an incident has occurred or is about to occur requiring quick and coordinated actions from a number of responders in order to minimize the impact of or prevent the event. In this situation, the responders, as part of the overall team monitoring the movement of DoD's cargo, are already connected to RAPID System. The idea is to make the collaboration environment a natural part of the responder's capability by making it an integrated part of the system. The events might unfold as follows.

Consider a normal movement of DoD cargo with all stakeholders and responders logged into RAPID System. An event occurs requiring immediate and coordinated responder attention. In today's world the responders would most likely begin by calling those they expect to work with to coordinate their activities. This is an important means of quick collaboration that should be maintained—at least in the near-term. However, when a number of responders try to call each other, busy signals can result, and, thus, delays in developing a coordinated approach. As a first step, RAPID Center could provide the responders with an emergency conference call number to facilitate this important step, one in which all responders, regardless of location, can participate.

Second, a text and graphics collaborative environment

could be added to RAPID System's capability to augment the conference call collaboration capability.

This facility would add features such as a whiteboard on which participants could draw or place overlays on which to draw. These overlays might be maps, drawings, or pictures that responders need to share with each other, discuss, or mark on to get points across. It should also provide a (text) chat feature, which should be downloadable by responders to create an actionable reference. Furthermore, it should be able to display pictures and streaming video from external sources (e.g., a plane flying over the tracks ahead of the train carrying the cargo). It should be possible to send material from the environment, or screen shots to external devices like mobile phones, which could keep all participants of the team in a closed loop.

We recognize that time is often shortest when collaboration is needed most. Therefore, setting up and participating in the environment should be extremely easy and intuitive. The initiator of a meeting should be able to establish a meeting, identify the participants, and specify the participants' permissions with a minimal number of clicks on a dropdown menu. Permissions should be changeable at any time. The default environment workspace should be designed to facilitate responder collaboration.

SOME COLLABORATIVE ENVIRONMENT CONSIDERATIONS

- Capabilities should include:
 - Whiteboard with overlay capability on which participants can draw
 - Chat and ability to download it for actionable reference
 - Ability to display pictures and streaming video from external sources
 - Ability to send screen shots of material being displayed to external devices
- Environment should be quick as well as easy to setup and to use
- Initiator of meeting should be able to easily set participants privileges before and during meeting
- A separate sign-on should not be required
- System should be able to protect data at the sensitive, but unclassified level

SOME COLLABORATIVE ENVIRONMENT CONSIDERATIONS (Continued)

Since, in general, participants would already be logged onto RAPID System, a mouse click or two is all that should be required for a participant to join an ongoing meeting. No separate logon should be required. The transition from the phone-only environment to that of the phone plus graphics should appear to the participants as seamless as possible.

Given that responders, the ultimate users of the data, can not be expected to have Federal Government security clearances, the system should be able to protect data at the sensitive, but unclassified level.

(This page is intentionally blank.)

SOME ISSUES NOT ADDRESSED

Because the goal of this appendix is to briefly describe possibilities for the future, a number of issues have not been addressed.

The capability of current communications systems to adequately support the different features of a virtual collaboration environment has not been examined. While this should not be a problem for upper echelons, it can be expected to be, at least in the near-term, for mobile units.

Security will remain a problem. As one tries to provide the responders with better and more complete data, one

runs into the security classification issue. For example, one can make a mobile phone secure, but how can one be sure the transmission is received in a secure environment? On the other hand, is the data so perishable or so urgently needed that it is worth the risk of compromise?

Resources and schedule are tied together as is often the case. They will be driven by how well one wishes to aid the responders.

SOME ISSUES NOT ADDRESSED

- Adequacy of communications
- Need for security
 - Center/system/workstation/mobile devices
 - User security clearances
 - Mobile users
- Resources
- Time/schedule

(This page is intentionally blank.)

Appendix E

GLOSSARY

Appendix E Glossary

AMC	Army Materiel Command	NCIS	Naval Criminal Investigation Service
BCS3	Battle Command Sustainment Support System	OSD	Office of the Secretary of Defense
CAP	civil air patrol	PA EMA	Pennsylvania Emergency Management Agency
C3I	command, control, communications, and intelligence	PA NG	Pennsylvania National Guard
CONUS	continental United States	PC	personal computer
COTS	commercial off-the-shelf	PKI	Public Key Infrastructure
		PRPA	Philadelphia Regional Port Authority
DBMS	database management system	R&D	research and development
DHS	Department of Homeland Security	RAPID	Regional Agile Port Intermodal Distribution
DLA	Defense Logistics Agency		
DoD	Department of Defense	SDD	Secure Data Device
DoT	Department of Transportation	SDDC	Surface Deployment and Distribution Command
DPO	Disaster Preparedness Office	SMS	short message service
DRMEC	Delaware River Maritime Enterprise Council	SSL	Secure Sockets Layer
DSCA	Defense Security Cooperation Agency		
DUSD	Deputy Under Secretary of Defense	TCN	transportation control number
		TDS	Tactical Data Systems
FBI	Federal Bureau of Investigation	THG	The Howland Group
		TRANSCOM	Transportation Command
ID	identification		
IDSS	Information Distribution Support System	ULN	unit line number
INS	Immigration and Naturalization Service		
ISC4	Information Systems Command, Control, Communications and Computers	VCE	Virtual Collaboration Environment
		WPS	Worldwide Port System
MARAD	Maritime Administration of the Department of Transportation		

(This page intentionally left blank.)

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YY) February 2006		2. REPORT TYPE Final		3. DATES COVERED (FROM - TO) September 2003–September 2005	
4. TITLE AND SUBTITLE The Development of RAPID System: From Concept to Initial Use and Beyond— Status Report				5A. CONTRACT NO.	
				5B. GRANT NO.	
				5C. PROGRAM ELEMENT NO(S).	
6. AUTHOR(S) Scheiber, L.B., Anstice, M.H., Hartka, J.E., Karrels, J.J., Miller, P.N., Smothers, E.R.				5D. PROJECT NO. ME1100, 1101, 1102	
				5E. TASK NO.	
				5F. WORK UNIT NO.	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882				8. PERFORMING ORGANIZATION REPORT NO. IDA Document D-3249	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Delaware River Maritime Enterprise Council Two Neshaminy Interplex, Suite 208 Trevose, PA 19053 ATTN: Ms. Susan Howland				10. SPONSOR'S / MONITOR'S ACRONYM(S) DRMEC	
				11. SPONSOR'S / MONITOR'S REPORT NO(S).	
12. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution unlimited.					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT The Federal Government has been working to increase the security of U.S. ports including the supply chains that move goods and material that pass through these ports. This is especially true in the case of war materiel moving between forts and depots in the United States and theaters of operation. In 2003, the Department of Transportation, Maritime Administration (DoT MARAD) tasked IDA to initiate an effort to help identify approaches to improve the safety and accountability of war materiel moving between forts and ships at the Port of Philadelphia. Beginning in 2004, the Delaware River Maritime Enterprise Council (DRMEC) tasked IDA to initiate the design, development, and demonstration of a pilot version of an online system to support tracking individual pieces of cargo, to provide a common operational picture to all stakeholders, and to provide RAPID Center with a means of alerting stakeholders to the occurrence or potential occurrence of significant events. The system, known as RAPID System, has been successfully used to support the return of war materiel as well as the deployment of a unit, the 10 th Mountain Division through the Port of Philadelphia. Modifications have been started to allow the system to support simultaneous operations involving multiple ships at multiple ports.					
15. SUBJECT TERMS systems, computers, collaboration, port, security, cargo, alerts, BCS3, counterterrorism, DRMEC, deployment, RAPID Center, RAPID System, wireless communications, mobile phones					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Unlimited	18. NO. OF PAGES 168	19A. NAME OF RESPONSIBLE PERSON Ms. Susan Howland
A. REPORT Unclassified	B. ABSTRACT Unclassified	C. THIS PAGE Unclassified			19B. TELEPHONE NUMBER (INCLUDE AREA CODE) (215) 633-7312